Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Музичука Дениса Сергійовича*

академічної групи *125-20-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Захист інформації на об'єктах критичної інфраструктури під час воєнного стану*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Ковальова Ю.В.			
розділів:				
спеціальний	доц. Ковальова Ю.В.	90б		
економічний	к.е.н., доц. Пілова Д.П.	90б		
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Музичуку Денису Сергійовичу* **академічної групи** *125-20-3*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Захист інформації на об'єктах критичної інфраструктури під час воєнного стану***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 р № 469-с

Розділ	Зміст	Термін виконання
Розділ 1	Структура об'єктів критичної інфраструктури. Вплив воєнного стану на зміни в об'єктах ОКІ.	15.03.2024
Розділ 2	Аналіз існуючих загроз та способи їх усунення. Варіанти покращення системи захисту та протидії загрозам на ОКІ.	10.05.2024
Розділ 3	Вартість та ефективність впровадження розроблених покращень для системи захисту інформації на ОКІ.	11.06.2024

Завдання видано _____ Юлія КОВАЛЬОВА
(підпис керівника) (ім'я, прізвище)

Дата видачі: 15.01.2024р.

Дата подання до екзаменаційної комісії: 28.06.2024р.

Прийнято до виконання _____ Денис МУЗИЧУК
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 95 с., 9 рис., 3 табл., 6 додатка, 33 джерел.

Об’єкт дослідження: системи захисту інформації на об’єктах критичної інфраструктури.

Мета роботи: Покращення і розробка ефективних методів і засобів захисту інформації на об’єктах критичної інфраструктури під час воєнного стану.

Методи дослідження: аналіз, порівняння, моделювання, синтез.

У першому розділі було досліджено теоретичні аспекти захисту інформації та визначено ключові поняття і терміни. Було проведено аналіз структури ОКІ та розібрано сучасні загрози і вразливості ІС об'єктів критичної інфраструктури в умовах воєнного стану.

У другому розділі розглянуто методи і засоби захисту інформації, що застосовуються, або застосовувалися, на об'єктах критичної інфраструктури. Було оцінено ефективність існуючих технологій та розроблено рекомендації щодо їх вдосконалення.

У третьому розділі було проведено розрахунки вартості та ефективності впровадження системи захисту інформації

Практична цінність розробки полягає у застосуванні розроблених методів і засобів для підвищення рівню захисту інформації на об’єктах критичної інфраструктури, зменшуючи ризик кібератак і збитків від них, що сприятиме підвищенню стійкості та безпеки держави під час воєнного стану.

Наукова новизна роботи полягає у розробці нових методів захисту інформації, адаптованих до умов воєнного стану.

ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, КІБЕРІНЦИДЕНТ, ОБ’ЄКТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ, КІБЕРАТАКА.

ABSTRACT

Explanatory note: 95 pp., 9 pic., 3 table, 6 app, 33 sources.

Research object: information protection systems at critical infrastructure facilities.

Purpose of work: Improvement and development of effective methods and means of protection information on critical infrastructure facilities during martial law.

Research methods: analysis, comparison, modeling, synthesis.

In the first chapter, theoretical aspects of information protection were investigated and key concepts and terms were defined. An analysis of the structure of the CIO was carried out and modern threats and vulnerabilities of IS of critical infrastructure objects in the conditions of martial law were analyzed.

In the second section, the methods and means of information protection that are used, or were used, at critical infrastructure facilities are considered. The effectiveness of existing technologies was evaluated and recommendations for their improvement were developed.

In the third section, calculations of the cost and effectiveness of the implementation of the information protection system were carried out

The practical value of the development lies in the application of the developed methods and means to increase the level of information protection at critical infrastructure facilities, reducing the risk of cyberattacks and damage from them, which will contribute to increasing the stability and security of the state during martial law.

The scientific novelty of the work consists in the development of new methods of information protection adapted to the conditions of martial law.

SECURITY POLICY, THREAT MODEL, VIOLATOR MODEL, INFORMATION SYSTEM, CYBER SECURITY, INFORMATION SECURITY MANAGEMENT, CYBER INCIDENT, CRITICAL INFRASTRUCTURE FACILITY, CYBER ATTACK.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ВС – воєнний стан;

ДСТУ – державний стандарт України;

ІКС – інформаційно-комунікаційна система;

КВОІ – критично важливий об’єкт інфраструктури;

КПЕ – ключові показники ефективності;

НСД – несанкціонований доступ;

ОКІ – об’єкти критичної інфраструктури;

ОС – операційна система;

ПЗ – програмне забезпечення.

СУІБ – система управління інформаційною безпекою;

ТЕС – теплова електростанція;

PAM – Privileged Access Management.

ЗМІСТ

ВСТУП

В сучасному світі та суспільстві, де інформація є ключовим ресурсом, захист інформації стає все більш важливим, особливо на об’єктах критичної інфраструктури. Під час воєнного стану, такі об’єкти стають особливо вразливими до кібератак, оскільки інформаційні системи стають однією з основних цілей кібернападів з боку противника, що може призвести до серйозних наслідків. Ефективний захист інформації на ОКІ стає ключовим елементом національної безпеки, що вимагає розробки та впровадження комплексних заходів і стратегій.

Актуальність роботи. Безпека інформації на об'єктах критичної інфраструктури є надзвичайно важливою складовою забезпечення національної безпеки. У сучасних умовах воєнного стану це завдання стає ще більш критичним через зростання ризиків та загроз з боку противника. Ефективний захист інформаційних систем на таких об'єктах дозволяє мінімізувати можливі втрати та забезпечити безперебійне функціонування життєво важливих процесів.

Об'єктами розробки у цій роботі являється об’єкти критичної інфраструктури, оскільки саме вони під час війни постраждали від різних типів атак більше всього. Структура систем ОКІ буде розглянута приблизно до правди, оскільки ці підприємства все ще є об’єктами критичної інфраструктури на які дуже важко отримати доступ.

Предметом розробки є системи захисту інформації на об’єктах критичної інфраструктури які будуть розроблятися виходячи з найкращих практик які використовуються за кордоном та які прописані законами і Державними Стандартами України.

Метою роботи являється дослідження впливу воєнного стану на ОКІ та розробка рекомендацій покращень захисту інформаційних систем.

Об’єктом дослідження є процеси захисту інформаційних систем на ОКІ в умовах війни та воєнного стану. Предметом дослідження є методи та технології захисту, державні та міжнародні стандарти захисту інформації.

Методи дослідження включають в себе аналіз сучасних державних та міжнародних стандартів ІБ, проведення досліджень впливу воєнного стану на ОКІ, а також розробка рекомендацій щодо покращення захисту ІС

Наукова новизна роботи полягає в вивчені та аналізі специфіки захисту інформаційних систем на ОКІ в умовах війни та воєнного стану. Практичне значення полягає у розробці рекомендацій та методів, завдяки яким може бути покращено захист інформації в інформаційних системах об'єктів КІ, підвищення стійкості до атак та інших загроз.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ.

1.1. Визначення та класифікація об’єктів критичної інфраструктури

Поняття критичної інфраструктури

Об’єкти критичної інфраструктури [1] – це об'єкти, які є надзвичайно важливими для функціонування суспільства та економіки країни. Безпека, цілісність та безперебійне функціонування цих об’єктів, як у нормальних умовах, так і в умовах надзвичайних ситуацій, таких як воєнний стан – один із найважливіших пріоритетів держави.

Згідно ЗУ «Про критичну інфраструктуру» [2], визначення терміну ОКІ наступе: це, об’єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди важливим національним інтересам.

Основні категорії об’єктів критичної інфраструктури

Об'єкти критичної інфраструктури є життєво важливими для безперебійного функціонування держави та суспільства. Згідно з Документом № 1109-2020-п [3], прийнятим Кабінетом Міністрів України, визначено порядок і критерії віднесення об'єктів до критичної інфраструктури. У цьому документі окреслено кілька ключових секторів, кожен з яких відіграє важливу роль у забезпеченні стабільності та безпеки країни. Нижче наведено список, який відображає основні сектори критичної інфраструктури та їхні ключові категорії:

1) Паливно-енергетичний сектор (Міненерго):

- електроенергетика: виробництво, ринок, передача, розподіл електроенергії, гідротехнічні споруди;
- вугільна промисловість: видобуток, зберігання вугілля;
- торфодобування: розробка родовищ, видобуток;
- нафтова промисловість: видобуток, передача, переробка нафти, нафтопроводи, зберігання;
- газова промисловість: видобуток, переробка, передача, розподіл газу, газотранспортна система;

– ядерна енергетика: виробництво палива, експлуатація установок, видобуток урану;

– енергетичне машинобудування: виробництво електрообладнання.

2) Цифрові технології (Мінцифри):

– електронні довірчі послуги та ідентифікація: надання послуг, функціонування систем;

– електронні комунікації: адміністрування, надання послуг;

– електронне урядування: функціонування систем взаємодії, надання адміністративних послуг.

3) Захист інформації (Держспецзв'язку):

– Кіберзахист.

4) Харчова промисловість та агропромисловий комплекс (Мінагрополітики):

– виробництво, переробка продукції, ветеринарні препарати, елеватори, зрошувальні системи.

5) Державний матеріальний резерв (Мінекономіки):

– зберігання запасів.

6) Охорона здоров'я (МОЗ):

– медична допомога: екстрена, первинна, спеціалізована, паліативна, реабілітація;

– громадське здоров'я: донорська кров, контроль інфекцій;

– фінансове забезпечення: оплата медпослуг;

– інформаційні технології: електронна система;

– фармацевтична промисловість: виробництво, забезпечення ліками.

7) Ринки капіталу та товарні ринки (НКЦПФР):

– функціонування ринків.

8) Фінансовий сектор (Мінфін):

– планування, моніторинг бюджетів, розрахунково-касове обслуговування, контроль податків, протидія відмиванню доходів, система гарантування вкладів, митні платежі.

9) Транспорт і пошта (Мінінфраструктури):

- авіаційний транспорт: управління рухом, перевезення, аеропорти;
- автомобільний транспорт: перевезення, будівництво доріг, контроль трафіка;
- метрополітен: перевезення пасажирів;
- залізничний транспорт: перевезення, обслуговування, вокзали;
- морський та водний транспорт: безпека, обслуговування суден, внутрішні шляхи, міжнародні зобов'язання;
- поштовий зв'язок: послуги пошти.

10) Системи життєзабезпечення:

- комунальні послуги: теплопостачання, гаряча вода, водопостачання, водовідведення, побутові відходи.

11) Промисловість (Мінстратегпром):

- хімічна промисловість: виробництво газів, добрив, пестицидів, вибухових речовин;
- металургія: гірничо-металургійний комплекс, виробництво коксу;
- оборонна промисловість: військова продукція;
- космічна промисловість: космічна техніка;
- авіаційна промисловість: продукція авіації;
- суднобудівна промисловість: суднобудування.

12) Громадська безпека (МВС):

- охорона порядку, критична інфраструктура, екстрена допомога 112.

13) Цивільний захист населення:

- реагування на надзвичайні ситуації, рятувальні служби.

14) Охорона навколишнього середовища (Міндовкілля):

- водні ресурси, поводження з радіоактивними відходами, охорона природних об'єктів, лісове господарство, управління відходами.

15) Оборона (Міноборони):

- зберігання та ремонт боєприпасів.

16) Правосуддя (ДСА):

– здійснення правосуддя.

17) Виконання кримінальних покарань (Мін'юст):

– тримання засуджених, військовополонених.

18) Державна реєстрація:

– інформаційні системи реєстрів.

19) Наукові дослідження та розробки (МОН)

– дослідницька інфраструктура, наукова діяльність.

20) Фінансовий сектор (Нацбанк):

– банківські послуги, зберігання готівки, небанківські фінансові послуги, платіжні послуги.

21) Вибори та референдуми (ЦВК):

– організація виборів, референдумів, інформаційні системи.

22) Соціальний захист (Мінсоцполітики):

– пенсійне забезпечення, соціальне страхування, допомога, інформаційні системи, реабілітація.

23) Інформаційний сектор (МКІП):

– телебачення, радіомовлення, видавнича сфера.

24) Державна влада та місцеве самоврядування:

– виконання функцій держави, місцеве самоврядування.

До переліку секторів критичної інфраструктури відносяться ті, які реалізують життєво важливі функції та/або послуги, порушення яких призводить до негативних наслідків для національної безпеки України, та має значний вплив на обслуговування населення, зокрема: урядування та надання найважливіших публічних (адміністративних) послуг, енергозабезпечення, водопостачання, продовольче забезпечення, охорона здоров'я та інші сектори, які перераховано у вищезгаданому документі.

Також, варто згадати, що об'єкти критичної інфраструктури поділяються на 4 категорії (1-4 у порядку спадання критичності) у відповідності до рівня їх важливості для забезпечення окремих життєво важливих функцій, в межах секторів критичної інфраструктури.

Існують такі категорії критичності об’єктів ОКІ[4]:

І категорія критичності – особливо важливі об’єкти, які мають загальнодержавне значення і значний вплив на інші об’єкти критичної інфраструктури, порушення функціонування яких призведе до виникнення кризової ситуації державного значення;

ІІ категорія критичності – життєво важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення;

ІІІ категорія критичності – важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення;

IV категорія критичності – необхідні об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення.

Процес категоризації об’єктів критичної інфраструктури проходить за наступною процедурою вказаною у Наказі від 15.01.2021 р. № v0023519–21 [5]:

1) секторальний орган у сфері захисту критичної інфраструктури ідентифікує всі об'єкти критичної інфраструктури свого сектору (підсектору) критичної інфраструктури згідно з Порядком віднесення об'єктів до критичної інфраструктури, затвердженим постановою Кабінету Міністрів України від 9 жовтня 2020 р. N 1109 "Деякі питання об'єктів критичної інфраструктури" (Офіційний вісник України, 2020 р., N 93, ст. 2994), – в редакції постанови Кабінету Міністрів України від 16 грудня 2022 р. N 1384;

2) секторальний орган у сфері захисту критичної інфраструктури відповідно до Порядку віднесення об'єктів до критичної інфраструктури для кожного об'єкта свого сектору (підсектору) критичної інфраструктури визначає, які основні послуги надає цей об'єкт;

3) секторальний орган у сфері захисту критичної інфраструктури разом із оператором критичної інфраструктури проводить оцінку критичності об'єкта критичної інфраструктури, використовуючи секторальні та міжсекторальні критерії визначення рівня негативного впливу, наведені у додатках Б і В, які враховують:

– рівень негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури;

– соціальну значущість об'єкта критичної інфраструктури;

– суспільну значущість об'єкта критичної інфраструктури;

– економічну значущість об'єкта критичної інфраструктури;

– наявність взаємозв'язків між об'єктами критичної інфраструктури;

– значущість об'єкта критичної інфраструктури для забезпечення національної безпеки та обороноздатності країни;

4) під час заповнення форми додатка 1 обирається рівень негативного впливу в рамках сектору або підсектору об'єкта критичної інфраструктури та у графі "Оцінка РКі" виставляється бал, який відповідає рівню негативного впливу, опис якого характеризує наслідки, які можуть настати у разі порушення функціонування об'єкта критичної інфраструктури;

5) під час заповнення форми додатка В обирається рівень негативного впливу за кожним критерієм, наведеним у формі, та у графі "Оцінка РКі" виставляється бал, який відповідає рівню негативного впливу, опис якого характеризує наслідки, які можуть настати у разі порушення функціонування об'єкта критичної інфраструктури;

6) підсумовуються всі бали, що були отримані під час оцінки об'єкта критичної інфраструктури згідно з формами, наведеними в додатках Б і В;

7) розраховується узагальнена нормована оцінка рівня критичності за формулою (1.1):

$$РК_{ОКІ} = \frac{\sum РК_i}{\sum РК_{max}} \qquad (1.1)$$

де $РК_{ОКІ}$ – узагальнена нормована оцінка рівня критичності об'єкта критичної інфраструктури;

$\sum РК_i$ – сума балів, які отримав об'єкт критичної інфраструктури за всіма критеріями критичності (додатки Б і В);

$\sum РК_{max}$ – максимальна можлива сума балів (розраховується виходячи з того, що об'єкт отримує максимальні бали за всіма критеріями оцінки рівня негативного впливу).

8) рішення щодо категорії критичності об'єкта критичної інфраструктури приймається на основі узагальненої нормованої оцінки рівня критичності об'єкта критичної інфраструктури відповідно до такого правила:

– I категорія критичності, якщо $0,8 < РКОКІ \leq 1$;

– II категорія критичності, якщо $0,63 < РКОКІ \leq 0,8$;

– III категорія критичності, якщо $0,37 < РКОКІ \leq 0,63$;

– IV категорія критичності, якщо $0,2 < РКОКІ \leq 0,37$;

– об'єкт не є критичним, якщо $РКОКІ \leq 0,2$;

9) підпункт 9 пункту 4 виключено

10) відомості про об'єкти критичної інфраструктури, що віднесені до I, II, III і IV категорії критичності, вносяться до секторального переліку об'єктів критичної інфраструктури, який формується та ведеться секторальним органом у сфері захисту критичної інфраструктури у відповідному секторі (підсекторі).

Розглянувши процес категоризації об’єктів критичної інфраструктури, вказаний вище, можна зрозуміти, що він є доволі комплексним і багатоступеневим, спрямованим на точну ідентифікацію і визначення оцінки критичності. Процедура забезпечує систематичний підхід, до захисту КІ, дозволяючи забезпечувати національну безпеку та ефективно управляти ризиками.

В цій роботі буде розглянуто об’єкти критичної інфраструктури з паливно–енергетичного сектору, а саме – електроенергетика, оскільки об’єкти цього сектору, зазвичай несуть великий вклад у роботу інших ОКІ. Тому будуть розглянуті саме об’єкти I і II категорій критичності, які належать до електроенергетичного сектору.

1.2. Вплив воєнного стану на об’єкти критичної інфраструктури

Захист об’єктів критичної інфраструктури є доволі важкою та відповідальною задачею, особливо під час воєнного стану, що передбачає повномасштабні бойові дії, обстріли та кібератаки. Усі ці загрози, мають багатогранний характер і можуть

бути фатальними для економіки, безпеки та добробуту населення. Основні типи загроз, під час ВС, можна поділити на такі категорії:

- фізичне знищення;
- перебої у постачанні;
- саботаж;
- диверсії;
- кібератаки.

Згідно дослідження Держспецзв'язку[6] сектори, які зазнали цілеспрямованих атак, залежність напрямів і впливу кібератак угрупування угрупування SANDWORM вказана на піраміді нижче (рис 1.1) і виглядає наступним чином:

Рисунок 1.1 – Піраміда залежності напряму і впливу кібератак угрупування SANDWORM

Основні загрози під час воєнного стану

Як вже було розглянуто раніше, є 5 категорій загроз які існують під час війни та які були перераховані раніше. В цьому пункті буде детально розглянуто кожну загрозу, способи їх реалізації та приклади їх використання в умовах активної агресії рф проти України, що триває.

Фізичне знищення

Фізичне знищення може передбачати безпосередні атаки на ОКІ, а саме, низку дуже небезпечних загроз, такі як бомбардування, ракетні удари, обстріли, атаки дронами та інші види фізичного руйнування.

Приклад 1: Пошкодження або руйнування електростанцій у ході бойових дій, що призводить до тривалих перебоїв в електропостачанні. Наприклад, під час конфлікту на сході України у 2014–2015 роках, коли рф проводила активні обстріли територій Донеччини. Або війна 24 лютого 2022 року, ступінь пошкодження наведена на рис. 1.2, коли росія почала бити по об'єктам критичної інфраструктури далеко за лінією бойового зіткнення в тилу, тим самим виводячи з ладу більшість електростанцій.

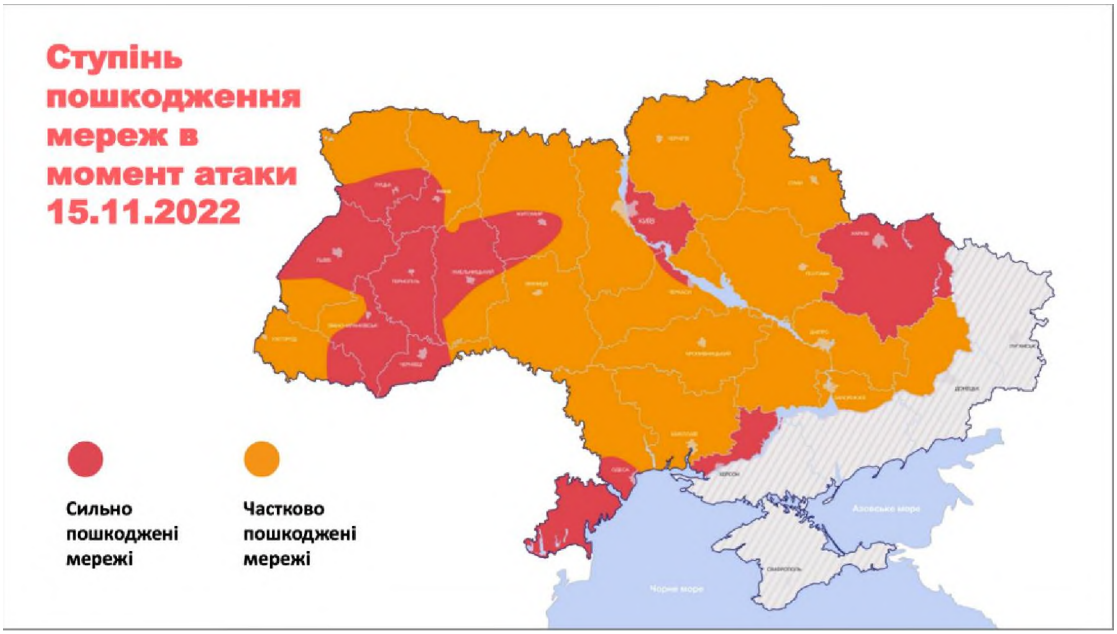

Рисунок 1.2 – Ступінь пошкодження мереж в момент атаки 15.11.2022[7]

Приклад 2: Під час воєнних дій, руйнування мостів, доріг та транспортних вузлів дуже ускладнює переміщення людей і товарів, особливо коли річ йде про звичайних цивільних. Саме так, під час воєнних дій у Сирії, були зруйновані

чисельні мости, що сильно ускладнило гуманітарні операції та постачання, необхідних для життя людей , товарів.

Якщо дивитися на цю загрозу через призму кібербезпеки та безпеки інформації в цілому, то можна зрозуміти що захистити сам об'єкт від загрози руйнування можуть тільки Збройні Сили України, а в наших силах, як експертів з кібербезпеки, можливо тільки захистити об'єкт від втрати інформації на електронних паперових та інших носіях інформації.

Перебої у постачанні

Перебої у постачанні, можуть виникнути за рахунок пошкоджень або знищення інфраструктури, яка забезпечує транспортування та розподіл критично важливих ресурсів, таких як газ, електроенергія, вода, продукти харчування або медикаменти. На деяких об'єктах ОКІ втрата тієї ж електроенергії або води, може призвести до часткової або взагалі повної зупинки роботи інфраструктури. Або ж ці ресурси можуть відрізнятися, наприклад для ТЕС, таким ресурсом може бути вугілля.

Приклад 1: Пошкодження газопроводів під час бойових дій може призвести до припинення постачання газу до промислових підприємств та житлових будинків, що створює серйозні проблеми, особливо у зимовий період. У 2022 році під час війни в Україні було пошкоджено кілька критично важливих газопроводів, що призвело до значних перебоїв у постачанні газу. Наприклад, унаслідок пошкодження магістрального газопроводу в Харківській області знижено тиск газу в газотранспортній мережі Донеччини [8]. Зниження тиску вплинуло на обсяги транспортування газу до об'єктів інфраструктури регіону.

Приклад 2: Знищення і пошкодження насосних, водозабірних станцій та систем водоочищення під час воєнний дій може призвести до дефіциту питної води для населення та звичайної води для об'єктів критичної інфраструктури. Під час громадянського конфлікту в Ємені у 2015–2016 роках [9], через воєнні дії зруйнована система охорони здоров'я та водопостачання й дезінфекції води. Ємценці були позбавлені найпростішого –можливості мити їжу та руки.

Якщо дивитися на цю загрозу через призму кібербезпеки та безпеки інформації в цілому, то можна зрозуміти що інформація в цьому випадку знаходиться під загрозою, тільки у випадку якщо ОКІ втратить доступ до електроенергії. В такому випадку експерти з кібербезпеки, мають можливість захистити тільки інформацію на електронних пристроях. Інші види інформації не знаходяться під загрозою.

Саботаж

Саботаж – це навмисні дії з метою пошкодження та/або виведення з ладу ОКІ зсередини, часто здійснювані агентами, шпіонами або зрадниками. Один з найкращих методів спротиву ворогу і як показує практика, ненасильницький підхід іноді, більш дієвій за акції прямої дії.

Приклад 1: Навмисне псування обладнання або продукції на електростанціях або заводах працівниками, що діють в інтересах ворога, може призвести до зупинки виробництва електроенергії та масових відключень. Наприклад, під час Другої світової війни були численні випадки саботажу на промислових підприємствах у країнах Європи і навпаки. Один із відомих випадків саботажу, було проведено компанією «Citroen» в умовах окупаційної війни [10]. Керівник заводу «Citroen», який на той час виготовляв одні з найкращих вантажівок Т45, розумів, що в разі відмови від співпраці, його просто замінять на лояльного до окупаційної влади. Тому він вирішив співпрацювати з окупантами та вести саботаж. Директор та інші працівники заводу, які долучились до саботажу, просто змінили конструкцію так званого «масляного щупа». Він показував, що рівень масла в двигуні достатній, хоча насправді він був менший за мінімально необхідний. В свою чергу призводило до передчасного виходу з ладу двигуна

Приклад 2: Підпали на складах з продовольством, снарядами або медикаментами, здійснені внутрішніми агентами ворога, можуть призвести до дефіциту життєво важливих ресурсів. У багатьох військових конфліктах світу застосовувалися такі дії, і призводили вони до серйозних наслідків як для цивільного населення, так і для ОКІ.

Якщо дивитися на цю загрозу через призму кібербезпеки та безпеки інформації в цілому, то можна зрозуміти що інформація в цьому випадку знаходиться під великою загрозою. Саботаж може бути націлений не тільки на виробничу складову ОКІ, а і на комп'ютерну або інформаційну частину. Через це загроза саботажу, буде розглянута дуже детально, оскільки з середини підприємства можна знищити інформацію абсолютно різними способами, їх буде ретельно розглянуто пізніше. Експерти з кібербезпеки, мають не допустити втрати, модифікації або перегляду інформації несанкціонованими особами.

Диверсії

Диверсія (лат. diversio – відхилення) – це дії спеціально підготовлених підрозділів (груп) або окремих осіб у тилу противника, спрямовані на виведення з ладу чи пошкодження шляхом підриву, підпалу або в ін. спосіб підприємств, доріг, засобів пересування, ОКІ та багато іншого.

Приклад 1: Знищення мостів, залізничних колій або інших транспортних об'єктів диверсійними групами можуть значно ускладнити логістичні операції та постачання військових та гуманітарних вантажів. Така практика використовується в абсолютно кожній війні, існують окремі диверсійні підрозділи які можуть прориватися в тил противника і наносити шкоду будь–яким ОКІ.

Якщо дивитися на цю загрозу через призму кібербезпеки та безпеки інформації в цілому, то можна зрозуміти що інформація в цьому випадку знаходиться під великою загрозою. Диверсія може бути націлений не тільки на виробничу складову ОКІ, а і на комп'ютерну або інформаційну частину. Загроза диверсії, буде розглянута дуже детально. Експертів з кібербезпеки, мають не допустити втрати, модифікації або перегляду інформації несанкціонованими особами.

Кібератаки

Кібератаки на критичну інфраструктуру стають дедалі серйознішою загрозою для всього світу. Кібератаки [11] спрямовані на пошкодження важливих документів і систем у корпоративній або персональній комп'ютерній мережі, а також отримання доступу до них. Кібератаки здійснюють як окремі особи, так і цілі

організації в політичних, кримінальних або особистих цілях для знищення засекреченої інформації чи отримання доступу до неї.

Нижче наведено кілька прикладів кібератак:

- зловмисні програми;
- розподілена атака "відмова в обслуговуванні" (DDoS–атака);
- фішинг;
- SQL–ін'єкції;
- міжсайтові сценарії (XSS);
- бот–мережі;
- зловмисні програми з вимогою викупу.

Приклад 1: Атаки хакерів на електронні мережі, які можуть призвести до масштабних відключень електроенергії, що призведе до проблем на інших ОКІ, на яких наявність електроенергії, невід'ємна частина їх функціонування. Наприкінці 2015 року Україна зазнала кібератаки на національну електромережу, в результаті чого понад 600 000 жителів залишилися без електрики [12]. 'Кібератаки на об'єкти критичної інфраструктури, які спостерігаються в останні роки, за своїм руйнівним потенціалом можна вважати зброєю масового ураження. Вочевидь, одним з основних напрямків оборонної стратегії держави має стати захист державних інформаційних ресурсів та систем від кіберзагроз та кібератак з боку інших держав та міжнародних злочинних хакерських угруповань.

Якщо дивитися на цю загрозу через призму кібербезпеки та безпеки інформації в цілому, то можна зрозуміти що інформація в цьому випадку знаходиться під великою загрозою. Кібератака як правило, націлена на комп'ютерну та інформаційну складову об'єкта, але за деяких умов, може торкнутися і виробничої частини підприємства. Загроза кібератаки, буде розглянута дуже детально. Це прямий обов'язок, експертів з кібербезпеки, не допустити втрати, модифікації або перегляду інформації несанкціонованими особами.

Вразливості об'єктів критичної інфраструктури у воєнний час

Об’єкти критичної інфраструктури можуть мати певний перелік вразливостей, які, в свою чергу, можуть бути використані зловмисниками, терористами або ворогом у ВС та які відрізняються для окремих ОКІ. Можна привести кілька прикладів базових вразливостей, які можуть існувати майже на кожному об'єкті критичної інфраструктури, не в залежності від їх категоризації або сектору:

– Використання централізованих систем управління: більшість ОКІ, використовують централізовані системи управління, що робить їх вразливими до сильних кібератак по одній точці. Виведення з ладу центральної системи, як правило, призводить до збоїв, або і взагалі повній зупинці підконтрольних об’єктів;

– Низький рівень обізнаності у сфері кібербезпеки: переважна більшість ОКІ мають доволі низький рівень кібербезпеки, особливо сильно на це впливає рівень обізнаності персоналу з основами кібербезпеки, що робить об’єкти легкою мішенню для хакерів. Застарілі системи та відсутність регулярних оновлень у системі значно підвищують вірогідність успішних атак;

– Відсутність систем резервного копіювання: недостатня кількість або і взагалі відсутність систем резервного копіювання, автоматизованого або ж ручного, може призвести до значних проблем та перебоїв у роботі системи після відбиття кібератаки, знищення якоїсь частини носіїв саботажем, диверсією або атакою ворожої армії по ОКІ.

1.3. Зміни в об’єктах критичної інфраструктури під час воєнного стану

Як правило, під час воєнного стану, ОКІ зазнають значних змін, націлених на підвищення їх базової стійкості, захищеності та безперебійності в умовах підвищених загроз. Особливу увагу приділяють захисту ІС та кібербезпеці, задля мінімізації ризиків і загроз потенційних кібератак.

Оновлення та модернізація систем безпеки

В умовах воєнного стану, значно зростає необхідність у модернізації або і повній заміні систем захисту інформації на ОКІ. Також це включає в себе впровадження новітніх технологій та покращення вже існуючих систем для підвищення їх стійкості до внутрішніх і зовнішніх загроз. Звісно ж, в наших реаліях

терористичної війни, з регулярними атаками дронами камікадзе і ракетами по об'єктам ОКІ, оновлення та впровадження новітніх систем може бути не тільки дорого, а ще й безцільно, оскільки одна атака і один випадковий уламок який потрапить у нову систему, може повністю її знищити. Саме тому, потрібно думати ще й про фізичну безпеку нових систем безпеки, що може бути досить важко, в залежності від об'єкта на якому вони впроваджуються.

Наприклад, значно підвищити рівень безпеки, можна впроваджуючи сучасні системи управління та моніторингу електромереж, які мають підвищену захищеність від кібератак. А саме, можна використовувати передові технології шифрування даних та багатофакторної аутентифікації для доступу систем управління тільки користувачам з наданими на це дозволами.

Також, обов'язковою частиною безперебійної роботи всіх підприємств, є регулярне оновлення ПЗ, що включає в себе встановлення останніх оновлень систем безпеки та впровадження систем виявлення(IDS) та запобігання кібератакам(IPS).

Посилення захисних заходів

Під час воєнного стану, посилення заходів захисту є критичним для забезпечення стабільної та безперебійної роботи ОКІ і мінімізації впливу кібератак. Посилення заходів кібербезпеки передбачає в собі впровадження технічних і організаційних рішень, що спрямовані на підвищення рівня захисту ІС на ОКІ. Нижче будуть приведені приклади заходів з кіберзахисту, які потрібно впровадити на об'єкті критичної інфраструктури, задля підвищення його стійкості і безпеки.

1) Технічні заходи:

– Впровадження багатофакторної автентифікація (MFA)

Опис: Багатофакторна автентифікація[13] (MFA) – це метод входу в систему, який вимагає від користувача підтвердження своєї ідентичності за допомогою кількох факторів автентифікації.

Наприклад, якщо ви використовуєте пароль для входу в свій обліковий запис, то Multifactor Authentication може додати до цього процесу ще один крок, як–от запит на код підтвердження, який буде надіслано на ваш мобільний телефон. Таким

чином MFA забезпечує додатковий бар'єр і рівень безпеки, який неймовірно складно обійти зловмисникам. MFA може блокувати понад 99,9 % атак компрометації облікового запису і є корисним для багатьох видів бізнесу.

– Застосування сучасних технологій шифрування

Опис: Шифрування[14] – це процес який полягає в перетворенні даних у незрозумілий формат, який може бути бути розшифрований лише за наявності ключа. Цей важливий процес, який дозволяє забезпечити безпеку та конфіденційність інформації в цифровому світі. Існують два основних види шифрування: симетричне та асиметричне.

Шифрування має широкий спектр застосувань, включаючи забезпечення безпеки інтернет–транзакцій, захист конфіденційних даних у сферах кібербезпеки та зберігання інформації, забезпечення безпечного обміну повідомленнями та захист фінансових операцій.

– Впровадження систем виявлення та запобігання вторгненням (IDS/IPS)

Система виявлення вторгнень [15] (СВВ) (Intrusion Detection System) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу (вторгнення або мережевої атаки) в комп'ютерну систему або мережу.

Система запобігання вторгненням (СЗВ) (Intrusion Prevention System)) – програмний або апаратний засіб, який здійснює моніторинг комп'ютерної системи в реальному часі з метою виявлення, запобігання або блокування шкідливої активності.

– Розгортання фаєрволів та VPN

Мережеві екрани (фаєрволи) контролюють вхідний та вихідний трафік, дозволяючи лише легітимні з'єднання, які були підтвердженні мережевим екраном, а віртуальні приватні мережі (VPN) забезпечують захищений канал для передачі даних та роботи підприємства через захищену мережу при цьому, не використовуючи публічні IP адреси, доступні через мережу інтернет.

Мережеві екрани, як правило, використовуються для захисту внутрішніх мереж об'єктів критичної інфраструктури та використання VPN для безпечного доступу до них з віддалених локацій.

– Регулярне оновлення програмного забезпечення

Своєчасні оновлення програмного забезпечення усувають вразливості та захищають системи від загроз, які щойно з'явилися і як правило виправляються розробником ПЗ, одразу після появи. Тому і важливо оновляти ПЗ регулярно і методично, одразу після виходу оновлень.

Як приклад, автоматичне оновлення ОС і прикладних програм на серверах та робочих станціях, що використовуються на ОКІ, важлива складова кібербезпеки підприємства.

1. Організаційні заходи

– Підготовка та навчання персоналу

В першу чергу, безпека інформації на підприємстві, або на ОКІ, залежить від того наскільки персонал знає і вміє користуватися своїм обладнанням. Якщо в обладнані персоналу, переважно домінують ПК, то задля підвищення обізнаності та компетенції співробітників, потрібно проводити навчальні програми та тренінги щодо кібербезпеки.

Наприклад, можна організувати щорічні тренінги з кібербезпеки для персоналу об'єктів критичної інфраструктури, включаючи симуляції кібератак та навчання правильним діям в разі інциденту.

– Розробка та впровадження політик кібербезпеки

На критично важливих об'єктах, дуже важливо встановити чіткі правила і процедури задля забезпечення захисту інформаційних систем і даних на них.

Наприклад, можна впровадити політику безпечного використання паролів. Це передбачає регулярну заміну та специфічні вимоги до складності пароля, що обов'язково для ОКІ.

– Створення команд реагування на інциденти (CERT–UA)

Також, можливе формування спеціалізованих груп, які будуть відповідальні за виявлення, аналіз та реагування на кіберінциденти. Окрім цього,

Наприклад, в Україні було створено команду CERT–UA [16] – Урядова команда реагування на комп'ютерні надзвичайні події України, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України.

– Розробка планів дій на випадок надзвичайних ситуацій (BCP/DRP)

План безперервності бізнесу (BCP) та план відновлення після катастроф (DRP), забезепечують готовність до відновлення функцій після інцидентів. Впровадження таких функцій має регламентуватися політиками безпеки і впроваджуватися на кожному підприємстві, задля безперебійної роботи та швидкого відновлення роботи після будь–якого інциденту безпеки.

– Проведення регулярних аудитів та тестування на проникнення (пентестів)

Регулярне оцінювання інформаційний систем на їй ступінь захищеності через аудити безпеки та проводення пентестів (Penetration Test) для виявлення та усунення вразливостей. Під час воєнного стану, пентести потрібно проводити або в ізольованому середовищі, або в симуляції системи, щоб не ослаблювати систему на випадок потенціальної атаки.

2) Комплексні заходи кіберзахисту

Поєднання технічних та організаційних заходів забезпечує створення багаторівневої системи захисту, яка є стійкою до різних видів загроз. Це включає:

Комплексні системи кіберзахисту, це поєднання організаційних і технічних заходів, які забезпечують створення багаторівневої системи захисту, яка є стійкою до різних типів загроз. В них входить:

– Введення систем виявлення та реагування в реальному часі на інциденти кібербезпеки. Впровадження систем SIEM (Security Information and Event Management) задля моніторингу, аналізу та реагування на інциденти.

Усі вищевказані заходи безпеки є ключовими для забезпечення безпеки інформаційних систем на ОКІ під час воєнного стану. Завдяки ним, ризики від кібератак будуть значно нижче, також буде забезпечена безперебійна робота та мінімізовані можливі наслідки від потенційних загроз.

1.4. Висновки до розділу

У цьому розділі було розглянуто вплив воєнного стану на ОКІ, розібрано термін ОКІ, на які сектори ОКІ поділяються та на які категорії. Також було приділено увагу методу категоризації ОКІ. Було вирішено об'єкти якого сектору та якої категорії критичності будуть розглядатися. А саме, об'єкти Паливно–енергетичного сектору, а саме електроенергетика. В ролі прикладів, будуть використані електроенергетичні об'єкти «ДТЕК», а саме «ПРИДНІПРОВСЬКА ТЕС».

Також в цьому розділі було розглянуто:

Ідентифікація загроз. Було розглянуто типи основних загроз під час воєнного стану, а саме фізичне знищення, перебої у постачанні, саботаж, диверсії та кібератаки. Усі ці загрози є дуже небезпечними і можуть спричинити порушення в роботі критичних систем та послуг.

Вразливості ОКІ. У кожного ОКІ, в методах захисту інформації є вразливості і сильні сторони. Важливо знаходити вразливості раніше ворога і укріпляти сильні сторони. Базовими прикладами вразливостей на ОКІ, які існують і по сьогоднішній день є застаріле обладнання, необізнаність персоналу з питань реагування на кіберзагрози, а також інші недоліки в ситемах безпеки. В умовах воєнного стану, усі ці загрози можуть бути використані задля здійснення атак, що підкреслює необхідність постійного моніторингу та оновлення заходів безпеки.

Вплив воєнних дій. Війна та воєнні дії мають прямий вплив на роботу ОКІ. Наприклад, прямі атаки по об'єктами, диверсії, диверсії у постачанні, або кібератаки, які можуть вивести з ладу системи управління або викрасти критично важливу інформацію. Це ще більше ускладнює і без того важкий захист ОКІ, тому важливо бути готовим до усього, особливо у ВС.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

Для покращення систем безпеки на ОКІ, потрібно більш детально розглянути існуючі загрози які з'являються під час воєнного стану, які існують завжди та які можуть з'явитися внаслідок проведення активних бойових дій. В цьому ж розділі, буде приділено більше уваги саме нейтралізації існуючих загроз, буде розглянуто більше прикладів кіберінцидентів які траплялися по всьому світу та шляхи, якими можна було б уникнути реалізації цих загроз.

Також буде розглянуто об'єкт критичної інфраструктури до якого і будуть розроблятися усі варіанти покращення систем захисту об'єктів критичної інфраструктури.

2.1.Опис системи і загальні відомості ОКІ підприємства «ДТЕК» у м. Дніпро

ДТЕК – це найбільша компанія з виробництва та відпуску електричної та теплової енергії, що входить до складу фінансово–промислової групи «Систем Кепітал Менеджмент» (скорочено «СКМ»). Компанія здійснює свою діяльність у сфері видобутку вугілля, виробництва електроенергії та її розподілу. ДТЕК обслуговує значну частину енергетичних потреб країни, забезпечуючи енергією мільйони споживачів.

ТЕК Енерго – ключовий гравець на ринку генерації електроенергії України, який виробляв чверть електроенергії в країні. Загальна встановлена потужність генерувальних об'єктів компанії перевищувала 13.527 МВт на момент 2021, до початку повномасштабної війни. ДТЕК Дніпроенерго – один із провідних виробників електроенергії та тепла в Україні. У складі компанії є три ТЕС, які розташовані в Запорізькій і Дніпропетровській областях, – Запорізька(5 травня 2022 р. електростанція зупинила роботу через те, що в умовах російської окупації закінчилося вугілля), Придніпровська, Криворізька. Встановлена потужність електростанцій компанії становила – 6 025 МВт.

Виробничі потужності компанії представлені підприємствами теплової генерації в складі ДТЕК Східенерго, ДТЕК Дніпроенерго, ДТЕК Західенерго.

Теплоелектростанції постачають усю вироблену електроенергію в оптовий ринок електроенергії України, за винятком Луганської ТЕС, яка входить до ДТЕК

Східенерго. Пошкодження магістральних електричних мереж НЕК «Укренерго» від'єднало ДТЕК Луганську ТЕС від Об'єднаної енергосистеми України. Станція з вересня 2014 року працює в режимі енергоострова.

У Дніпропетровській області, ДТЕК Дніпроенерго представлений кількома ключовими об'єктами критичної інфраструктури, зокрема[16]:

1) Шахтоуправління імені Героїв Космосу, Дніпропетровська область, Павлоградський район, с. Вербки. До складу шахтоуправління ім. Героїв космосу входять дві шахти: ім. Героїв космосу та Павлоградська. Це найбільше шахтоуправління в об'єднанні ДТЕК Павлоградвугілля за річним обсягом видобутку вугілля.

2) Шахтоуправління Дніпровське, Дніпропетровська область, Павлоградський район, с. Шахтарське. До складу шахтоуправління Дніпровське входять дві шахти: Самарська та Дніпровська. На шахтоуправлінні працюють мешканці найбільшої кількості населених пунктів Західного Донбасу. Щодня сюди приїжджають працівники з 42 міст, селищ та сіл.

3) Шахтоуправління Тернівське, Дніпропетровська область, м. Тернівка. Шахтоуправління Тернівське – одне з найбільших вуглевидобувних підприємств ДТЕК Енерго, до складу якого входять дві шахти – Західно–Донбаська (що працює двома блоками) та Тернівська. За роки роботи тут видобули понад 130 млн тонн вугілля, підготували до роботи понад 1,2 тис. км гірничих виробок.

4) Шахтоуправління Першотравенське ,Дніпропетровська область, Синельниківський район, м. Першотравенськ. До складу шахтоуправління входять дві шахти: Степова та Ювілейна. Видобутком та підготовкою нових гірничих виробок на шахтоуправлінні займаються вісім виробничих дільниць. Організовують їхню роботу ще 27 допоміжних колективів.

5) Корум Дружківський машинобудівний завод Дніпропетровська область, м. Дніпро. Корум Дружківський машинобудівний завод – це 130 років досвіду, досягнень, професіоналізму та славної історії! Нині, Корум Дружківський машинобудівний завод – флагман гірничошахтного машинобудування України!

6) Криворізька ТЕС, Дніпропетровська область, Криворізький район, м. Зеленодольськ. ДТЕК Криворізька ТЕС – єдина станція в Україні, яка може працювати на трьох видах вугілля. Проєктне паливо Криворізької ТЕС – пісне вугілля, та завдяки модернізації обладнання станція може працювати ще й на газовому вугіллі та на суміші газового й антрациту.

7) ЦЗФ Павлоградська, Дніпропетровська область, Павлоградський район, с. Вербки. Центральна збагачувальна фабрика Павлоградська – найбільше і одне із найсучасніших вуглезбагачувальних підприємств України, яке «перетворює» видобуту шахтами гірничу масу на вугільний концентрат. Фабрика безперебійно забезпечує паливом кілька теплових електростанцій, завдяки чому українські міста отримують електроенергію.

8) Придніпровська ТЕС, Дніпропетровська область, м. Дніпро. ДТЕК Придніпровська ТЕС має 69–річну історію. Свого часу вона стала основою і стимулом розвитку промисловості регіону. Станція, спочатку спроектована для роботи на антрацитовому вугіллі, зараз переобладнана для роботи на українському газовому вугіллі, а отже, сприяє енергобезпеці країни.

9) Першотравенський ремонтно–механічний завод, Дніпропетровська область, Синельниківський р–н, с. Миколаївка. Першотравенський ремонтно–механічний завод ремонтує гірничо–шахтне обладнання, виготовляє деталі до нього та аркове кріплення для шахт.

10) Павлоградвантажтранс, Дніпропетровська область, м. Павлоград. Філія ДТЕК Павлоградвугілля Павлоградвантажтранс доставляє вугілля з шахт на теплоелектростанції країни.

11) Павлоградське енергопідприємство, Дніпропетровська область, м. Павлоград. Павлоградське енергопідприємство забезпечує гарячою водою та теплом багатотисячний колектив підприємств ДТЕК Павлоградвугілля.

12) Соцвугілля, Дніпропетровська область, м. Павлоград Співробітники філії ДТЕК Павлоградвугілля Соцвугілля організовують відпочинок працівників підприємств та їхніх родин, готують смаколики, організовують проживання, забезпечують побутовим паливом робітників та пенсіонерів компанії.

13) Павлоградське управління з матеріально–технічного постачання, Дніпропетровська область, м. Павлоград. Павлоградське управління з матеріально–технічного постачання забезпечує підприємства ДТЕК Енерго усіма необхідними для ефективної роботи матеріалами та обладнанням – від канцелярської скріпки до гірничовидобувної техніки.

14) Павлоградська автобаза, Дніпропетровська область, м. Павлоград. Павлоградська автобаза – одне з найбільших автопідприємств України. Має 5 автомобільних колон та дві колони дорожньо–будівельної техніки у Дніпропетровській та Донецькій областях.

15) Сервісно–налагоджувальне управління, Дніпропетровська область, м. Павлоград. Філію Сервісно–налагоджувальне управління утворено в 2022 році на базі ДТЕК Павлоградвугілля. СНУ є одним з найсучасніших спеціалізованих підприємств України з сервісного обслуговування, ремонту гірничо–шахтного, стаціонарного, високовольтного обладнання, високовольтних електродвигунів.

Також дуже важливо підмітити, що усі об’єкти критичної інфраструктури, працюють тільки завдяки Криворізькій ТЕС, Придніпровській ТЕС та імпортованій енергії з країн заходу. Наразі, навіть під час війни і регулярних стабілізаційних відключень електроенергії, ОКІ використовують більшу частину світла, аніж населення, бізнес та об’єкти соціально–побутової сфери у Дніпропетровській області. Згідно даним які були надані ДТЕК, діаграму наведено на рис 2.1, ОКІ споживають 57% електроенергії яка виготовляється та імпортується[17].

Рисунок 2.1 – Діаграма споживання електроенергії у Дніпропетровській області

Енергетичний сектор ОКІ неймовірно важливий, особливо для інших критично важливих об'єктів інфраструктури, яких існує дуже багато у Дніпропетровській області. Тому роботою передбачається саме огляд і аналіз ОКІ ДТЕК Придніпровська ТЕС, який є одним із ключових поставників електроенергії, а також наведення варіантів покращення систем захисту на цьому об'єкті ОКІ.

Придніпровська ТЕС та майже кожен об'єкт ДТЕК складаються з наступних елементів інформаційної структури:

1) Application Server (AS) – сервер на якому проводиться обробка та накопичення інформації;

2) Historian Server (HS) – сервер на якому зберігаються архівні дані та дані для бекапу;

3) Information Server (IS) – резервний сервер з обробки та накопичення інформації, який має додаткову функції відображення інформації у реальному часі та архівних даних із застосуванням веб–інтерфейсу;

4) Велика кількість корпоративних ПК робітників та декілька автоматизованих робочих місць операторів.

Також на деяких підприємствах ДТЕК, використовувався віртуальний сервер для газовидобутку [18]. Тобто, сервер був створений для фахівців з геології та розробки, для будування 3D–моделювання родовищ. Використовуючи програмний комплекс “Petrel” працівники виконують роботу з даними більше ніж сотні гігабайтів.

2.2.Аналіз та класифікація існуючих загроз безпеці об’єкта критичної інфраструктури

Під час воєнного стану, усі можливі ризики значно зростають. Важливо мати чітке уявлення природи існуючих загроз, вірогідні наслідки та їхні джерела. Це дає змогу активно запобігати їм, знижуючи потенційний вплив на критичні об’єкти, а не просто реагувати на інциденти які вже відбулися. Враховуючи те, що усі загрози можуть бути як навмисними так і випадковими, внутрішніми та зовнішніми, технічними та людськими, їх систематизація є необхідною для існування міцної та надійної системи захисту інформації.

Нижче, в цьому підрозділі, будуть розглянуті основні типи загроз інформаційній безпеці на ОКІ, що дозволить глибше розуміти їх специфіку та варіативність і розробити методи протидії цим загрозам. Класифікація загроз за джерелами їх походження, природою та характером впливу, забезпечить комплексний підхід до аналізу та управління ризиками, що виникають у сфері кібербезпеки ОКІ.

Отже, загрози безпеці інформації в ІС на ОКІ можна класифікувати за їх впливом на інформацію. У випадку реалізації можливих загроз інформації, є порушення інформаційної безпеки, тобто порушення конфіденційності, цілісності, доступності і неспростовності інформації, що абсолютно недопустимо у випадку з об’єктами КІ.

Розрізняють чотири типи загроз безпеки інформації:

- несанкціонований доступ до інформації;
- несанкціоновані зміни або викрадення інформації;
- відмова в обслуговуванні або профілактика авторизованого доступу;
- відмова у визнанні участі, авторства або відмова від одержання.

Тобто, конфіденційність буде забезпечена у випадку дотримання встановлених правил доступу до системи; цілісність – якщо будуть дотримані встановлені правила доступу до системи; доступність – якщо зберігається можливість доступу до системи або модифікації інформації, відповідно до встановлених правил упродовж певного, як правило малого проміжку часу; неспростовність – якщо факт участі в події що трапилась, причетність до утворення або передачі будь якого документа чи повідомлення, причетність до одержання будь–якого документа або повідомлення буде зафіксована.

Загрози для ІС ОКІ можуть виходити з різноманітних джерел:

– навмисних (терористичні групи, війна та військові конфлікти, промислові шпигуни, невдоволені працівники, зловмисники);

– ненавмисних (складність системи, людські помилки, аварії, відмови обладнання);

– природних (стихійні лиха, кліматичні умови тощо).

Якщо існує загроза, то є і можливість її реалізації – атака. Атака – це спроба знищення, розкриття внесення змін, пошкодження, викрадання або отримання несанкціонованого доступу до активу [19]. Прикладом несанкціонованого внесення змін є маніпулювання технологічною інформацією, що циркулює в ІС ОКІ. Тобто зміна даних, які передаються від датчика до програмованого логічного контролера (ПЛК) або зміна керуючого впливу від програмованого логічного контролера до виконавчого пристрою. Також можливі атаки типу "відмова в обслуговуванні", дія яких спрямована на компоненти ІС ОКІ або лінії зв'язку, і які можуть бути навмисними або спричиненими відмовами обладнання. Атаки такого типу можуть призвести до неможливості подальшого керування технологічним процесом і до його вимушеної зупинки. У тому випадку, коли цикл виробництва підприємства повинен бути безперервним, це призведе до збитків, які будуть викликані простоєм виробництва і повторним запуском технологічного процесу.

Оцінка ризику є дуже важливим компонентом цілісного процесу управління ризиками в масштабах всієї організації, як визначено в спеціальній публікації NIST 800–39 «Управління ризиками інформаційної безпеки: погляд на організацію, місію

та інформаційну систему» [20]. Управління ризиками – це складна, багатогранна діяльність, що вимагає залучення всієї організації – від вищих керівників, які забезпечують стратегічне бачення та цілі найвищого рівня і цілі організації; до лідерів середнього рівня, які займаються плануванням, виконанням і управлінням проектів; та особам на безпосередньому виробництві, які керують інформаційними системами, що підтримують місії/ділові функції організації. Технологічні засоби захисту

Процеси управління ризиками включають: визначення ризику; оцінка ризику; реагування на ризик; та моніторинг ризику. Рисунок 2.2 ілюструє чотири кроки у процесі управління ризиками, включаючи етап оцінки ризиків та інформаційні та комунікаційні потоки, необхідні для ефективної роботи процесу.

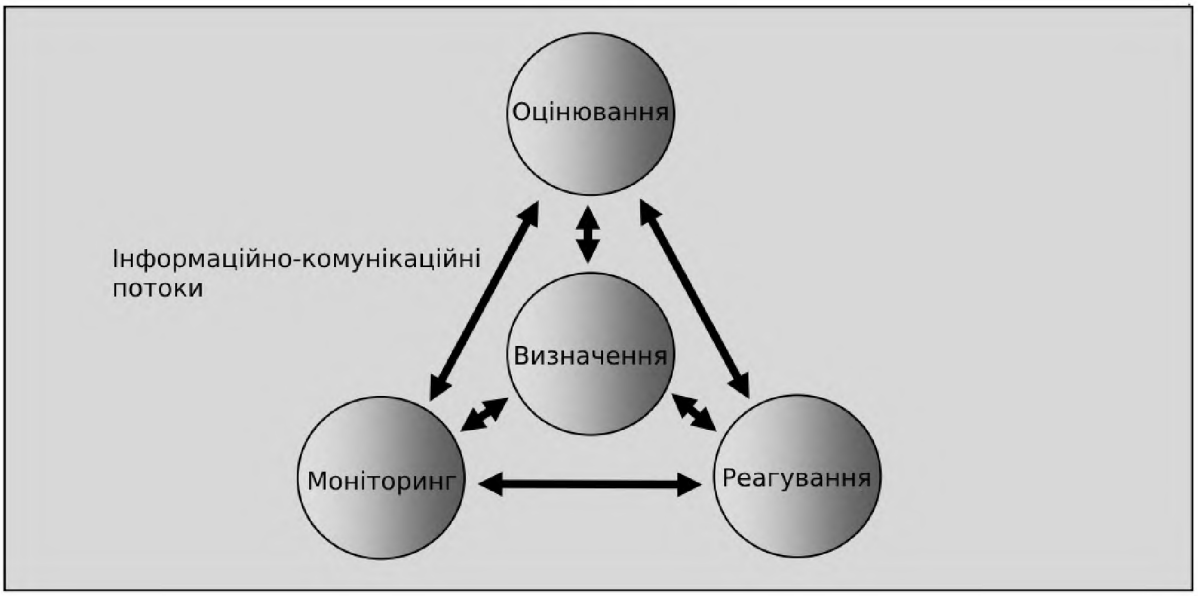

Рисунок 2.2 –Оцінка ризиків в процесі управління ризиками

Перший компонент управління ризиками стосується того, як організації формують ризик або встановлюють контекст ризику, тобто опис середовища, в якому приймаються рішення на основі ризику. Метою компонента формування ризику є розробка стратегії управління ризиками, яка стосується того, як організації мають намір оцінювати ризик, реагувати на ризик і контролювати ризик, роблячи чіткими та прозорими уявлення про ризик, які організації регулярно використовують під час прийняття як інвестиційних, так і операційних рішень.

Стратегія управління ризиками встановлює основу для управління ризиками та окреслює межі для рішень, що ґрунтуються на ризиках в організаціях.

Другий компонент управління ризиками стосується того, як організації оцінюють ризики в контексті системи організаційних ризиків. Метою компонента оцінки ризику є виявлення:

– загроз для організацій (тобто операцій, активів або окремих осіб) або загроз, спрямованих через організації проти інших організацій або країни;

– внутрішні та зовнішні вразливості організацій;

– шкода (тобто несприятливий вплив), яка може виникнути з огляду на потенціал загроз, що використовують уразливості;

– ймовірність заподіяння шкоди. Кінцевим результатом є визначення ризику (тобто, як правило, функція ступеня шкоди та ймовірності заподіяння шкоди).

Третій компонент управління ризиками стосується того, як організації реагують на ризик, коли цей ризик визначено на основі результатів оцінки ризику. Метою компонента реагування на ризик є забезпечення узгодженої відповіді на ризик у масштабах всієї організації відповідно до організаційної системи ризику шляхом:

– розробки альтернативних курсів дій для реагування на ризик;

– оцінка альтернативних варіантів дій;

– визначення відповідних напрямків дій, які відповідають толерантності організаційного ризику; та

– впровадження реагування на ризики на основі вибраних курсів дій.

Четвертий компонент управління ризиками стосується того, як організації здійснюють моніторинг ризиків у часі. Метою компонента моніторингу ризиків є:

– визначення поточної ефективності реагування на ризики (відповідно до організаційної системи ризиків);

– визначити зміни, що впливають на ризики, в організаційних інформаційних системах та середовищах, у яких ці системи працюють;

– перевірити, чи впроваджуються заплановані заходи реагування на ризики, а вимоги щодо інформаційної безпеки, які випливають із організаційних

місій/ділових функцій, федерального законодавства, директив, правил, політик, стандартів і вказівок, виконуються.

За джерелами походження загрози для об'єктів КІ поділяються на:

1) Внутрішні загрози

Однією з найбільш небезпечних і складних категорій загроз, є внутрішні загрози. Ці загрози походять від людей які мають легітимний доступ до внутрішніх систем ОКІ, що робить їх надзвичайно складними для виявлення і попередження. Ці загрози можуть бути реалізовані як навмисними діями, так і ненавмисними помилками працівників, підрядників або інших осіб, що мають доступ до критичних систем та інформації.

Види внутрішніх загроз:

– Зловмисні дії (Malicious insiders):

Незадоволений працівник, в цілях помсти, зиску чи бажання отримання винагороди від конкурентів або ворога, може навмисно пошкодити, видалити або модифікувати важливі файли, заразити систему шкідливим ПЗ або вкрасти і передати конфіденційну інформацію конкурентам або ворогам.

Згідно з опитуванням проведеним «Gurucul» [21], кожен четвертий працівник викрав би інформацію про компанію, щоб отримати роботу в конкуруючій фірмі. Згідно з опитуваними 476 професіоналами з IT–безпеки, майже кожен четвертий (24%) сказав, що візьме інформацію про компанію, щоб допомогти подати заявку на посаду в фірмі конкурента. Дослідження також виявило, що постачальники керованих послуг (34%) і розробники (30%) є основними джерелами ризику для третіх сторін, і що якщо хтось вчинить шахрайство, це, швидше за все, станеться у фінансовому відділі (32%);

– Недбалість або помилки (Negligent insiders):

Припустимо ситуацію, співробітник випадково відкриває фішинговий електронний лист, що призводить до встановлення шкідливого ПЗ на комп'ютер, який має доступ до критичних даних. Це дуже небезпечно, оскільки відкриває доступ до корпоративної мережі злочинцям, і призводить до порушення конфіденційності інформації, та можливо її цілісності і доступності.

Згідно з дослідженням, проведеним IBM [22], помилки людей є одними з головних загроз безпеці для компаній. Це пояснюється тим, що порушення, пов'язані з людськими помилками, потребують більше часу для локалізації та можуть призвести до ескалації збитків. Серед головних причин порушень безпеки людські помилки спричинили майже 90 відсотків загальної кількості порушень у 2019 році. Крім того, людські помилки спричинили 60 відсотків усіх порушень у 2018 році та 68 відсотків порушень у 2019 році. На ці сектори припадає 23,8% інцидентів безпеки, а решта були спричинені випадковими помилками або зловмисними діями працівників.

– Зловживання доступом (Abuse of access):

Адміністратор системи використовує свої привілеї для доступу до конфіденційної інформації з особистих або фінансових мотивів, наприклад, для продажу цієї інформації третім особам.

Організації впроваджують «privileged access management» або PAM [23](керування привілейованим доступом) для захисту від загроз, пов'язаних із крадіжкою облікових даних і зловживанням привілеями. PAM відноситься до комплексної стратегії кібербезпеки, що включає людей, процеси та технології, щоб контролювати, відстежувати, захищати та перевіряти всі привілейовані ідентифікаційні дані та дії людей і нелюдей у IT–середовищі підприємства.

PAM, який іноді називають керуванням привілейованою ідентифікацією («privileged identity management», PIM) або безпекою привілейованого доступу («privileged access security», PAS), базується на принципі найменших привілеїв, згідно з яким користувачі отримують лише мінімальний рівень доступу, необхідний для виконання своїх службових функцій. Принцип найменших привілеїв широко вважається найкращою практикою кібербезпеки та є фундаментальним кроком у захисті привілейованого доступу до цінних даних і активів. Застосовуючи принцип найменших привілеїв, організації можуть зменшити площу атаки та зменшити ризики з боку зловмисних інсайдерів або зовнішніх кібератак, які можуть призвести до дорогого витоку даних. Збільшення рівню безпеки в цій області дуже важливо, оскільки збитки через такі примітивну помилки, можуть бути невипраними.

Заходи для протидії внутрішнім загрозам:

– Моніторинг та аудит:

Моніторинг активності користувачів (UAM) [24]– технічна можливість спостерігати та записувати дії та активність особи в будь–який час на будь–якому пристрої, який отримує доступ до критично важливої інформації на ОКІ, щоб виявити внутрішні загрози та підтримати розслідування. Використання систем моніторингу для виявлення аномальної поведінки в мережі та проведення регулярних аудитів безпеки для виявлення потенційних внутрішніх загроз.

Нижче наведено деякі з областей, які слід враховувати, коли ви розробляєте індикатори UAM і тригери для моніторингу та звітності. На рисунку 2.3 нижче, зображено деякі потенційні показники ризику, які може виявити UAM.

Рисунок 2.3 – Потенційні показники ризику

– Навчання та підвищення обізнаності:

Проведення регулярних тренінгів з кібербезпеки для підвищення рівня обізнаності співробітників, щодо внутрішніх загроз та навчити розпізнавати ознаки підозрілої поведінки.

Навчання з питань безпеки є важливим компонентом комплексної програми безпеки. Без відповідного контенту людям, які не мають технічного досвіду, важко дотримуватись нормативних вимог і змінювати поведінку. SANS Security Awareness [25] пропонує комплексне рішення для користувачів і окремих осіб усіх рівнів із контентом, створеним експертами. Ця партнерська програма, створена надійною глобальною мережею професіоналів з кібербезпеки, включає кілька ключових продуктів для підвищення обізнаності про безпеку:

– кінцевий користувач – комплексне навчання з питань безпеки для всього персоналу, розроблене фахівцями галузі, щоб змінити поведінку користувачів, вдосконалити вашу програму та захистити вашу організацію;

– інструменти фішингу – постійно підкреслюйте важливість безпеки та створюйте першокласний захист від будь–яких видів фішингових атак;

– іт–адміністратор – підвищте рівень свого технічного персоналу за допомогою поглибленого навчання, щоб захистити всю вашу організацію;

– розробник – навчіть своїх розробників безпечним методам кодування та тому, як розпізнавати поточні вектори загроз у веб–додатках;

– nerc cip – відповідне навчання стосується стандартів надійності nerc cip для комунальної галузі;

– інженер ics – розроблено виключно для людей, які підтримують, взаємодіють із середовищами ics або працюють у них;

– Контроль доступу:

Впровадження багаторівневих систем контролю доступу, які обмежують доступ до критичних систем та інформації лише тим співробітникам, які дійсно потребують цього для виконання своїх обов'язків [26].

Рішення щодо контролю доступу часто визначаються ролями, які окремі користувачі виконують в організації. Це включає в себе визначення обов'язків, відповідальності та кваліфікації. Наприклад, особи, пов’язані з лікарнею, можуть виконувати такі ролі, як лікар, медсестра, клініцист і фармацевт. Ролі в банку включають касира, кредитного спеціаліста та бухгалтера. Ролі також можуть стосуватися військових систем; наприклад, аналітик цілі, аналітик ситуації та

аналітик трафіку є типовими ролями в тактичних системах. Політика керування доступом на основі ролей («Role–based access control» – RBAC) ґрунтує рішення щодо керування доступом на функціях, які користувач може виконувати в організації. Користувачі не можуть передавати права доступу іншим користувачам на свій розсуд.

Ролі орієнтовані на групу. Для кожної ролі зберігається набір транзакцій, призначених ролі. Транзакцію можна розглядати як процедуру перетворення (програму або частину програми) плюс набір пов'язаних елементів даних. Крім того, кожна роль має пов'язаний набір окремих учасників. У результаті RBAC надають засоби іменування та опису зв'язків «багато–до–багатьох» між особами та правами. На рисунку 2.4 зображено зв'язки між окремими користувачами, ролями/групами, процедурами трансформації та системними об'єктами.

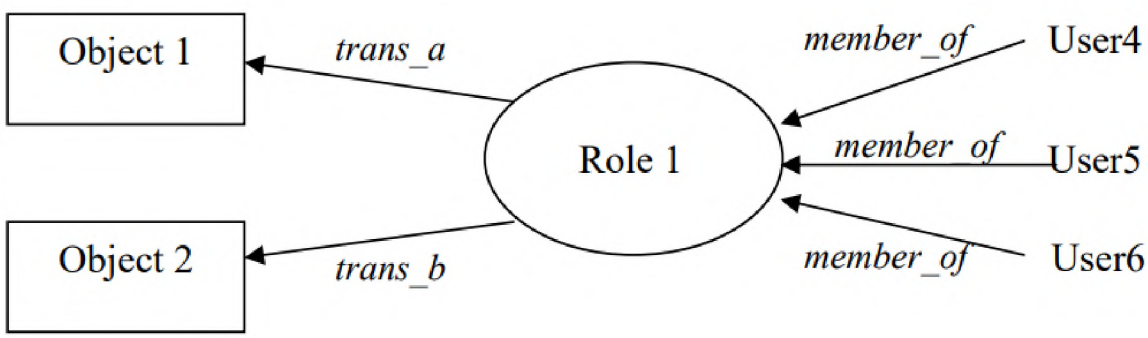

Рисунок 2.4 – Зв'язки між окремими користувачами, ролями/групами, процедурами трансформації та системними об'єктами

– Управління привілеями:

Обмеження привілеїв доступу до критичних систем, забезпечення, щоб користувачі мали лише ті права, які необхідні для їхньої роботи, та регулярний перегляд цих прав.

Принцип найменших привілеїв є фундаментальною концепцією кібербезпеки в багатьох публікаціях NIST, включаючи NIST 800–53 [27]. Це гарантує, що люди мають лише права та дозволи, необхідні для виконання своїх ролей і обов'язків,

щоб запобігти несанкціонованому доступу, випадковому пошкодженню через помилки користувача та зловмисним діям.

Принцип найменших привілеїв не застосовується лише до IT–користувачів. Він поширюється на ідентифікатори програмного забезпечення та машин, гарантуючи, що програми, облікові записи служб, API та автоматизовані процеси мають мінімально необхідні привілеї.

За принципом найменших привілеїв ви:

– Надав користувачам мінімальний рівень доступу необхідний для виконання їхніх службових функцій, ви:

– Обмежуєте доступ до конфіденційної інформації та критичних систем.

– Розділюєте обов'язки, щоб підтримувати систему стримувань та противаг.

– Регулярно переглядайте та оновлюйте привілеї доступу.

Дотримання принципу найменших привілеїв покращує загальну безпеку за рахунок зменшення поверхні атаки.

Висновок

Внутрішні загрози є дуже важкими для виявлення та попередження, та несуть велику небезпеку для ОКІ. Ефективна боротьба з цими загрозами, вимагає комплексного підходу, а саме ряд організаційних, освітніх та технічних заходів. Регулярне впровадження такого роду заходів, знижає ризики пов’язані з внутрішніми загрозами та забезпечує надійний захист КВОІ.

2) Зовнішні загрози

Більшість загроз виникають за межами організації і становлять значний виклик безпеці ОКІ. Причини з яких вони можуть бути спричинені, різні. Наприклад це можуть бути хакери, конкуренти або інші зацікавлені в цьому сторони, цілями яких це завдання шкоди, отримання конфіденційної інформації або порушення стабільності роботи підприємства. Як правило, ці загрози є дуже небезпечними через свою непередбачуваність та складність у виявленні.

Види зовнішніх загроз:

– Кіберзлочинність і кібершпигунство (Cybercrime and cyber espionage):

Щомісяця викрадається понад 10 терабайт даних, програми–вимагачі все ще вважаються однією з головних загроз у новому звіті, а фішинг зараз визначено як найпоширеніший початковий вектор таких атак. Іншими загрозами, які займають найвище місце серед програм–вимагачів, є атаки на доступність, які також називаються розподіленими атаками на відмову в обслуговуванні (DDoS).

Проте геополітична ситуація, зокрема російське вторгнення в Україну, за звітний період змінила правила глобальної кіберсфери. Хоча все ще спостерігається збільшення кількості загроз, також можна помітити, що з'являється ширший спектр векторів, таких як експлойти нульового дня, дезінформація та глибокі фейки за допомогою ШІ. У результаті з'являються більш зловмисні та поширені атаки, які мають більш руйнівний вплив.

Виконавчий директор Агентства ЄС з кібербезпеки Юхан Лепассар заявив [28], що «сучасний глобальний контекст неминуче спричиняє серйозні зміни в ландшафті загроз кібербезпеці. Нова парадигма формується зростаючим колом учасників загрози. Ми вступаємо у фазу, яка потребуватиме відповідних стратегій пом'якшення наслідків для захисту всіх наших критичних секторів, наших галузевих партнерів і, отже, усіх громадян ЄС».

– Кібертероризм (Cyber terrorism):

Приклад: Терористичні групи використовують кіберзасоби для атак на критичну інфраструктуру з метою створення паніки, дестабілізації та завдання економічної шкоди. Це може включати атаки на енергетичні системи, транспортні мережі, водопостачання тощо.

Кібертероризм, як зазначено в дослідженні «Cyberterrorism as a global threat: a review on repercussions and countermeasures» написаного автором Saman Iftikhar [28], означає використання інтернету, інформаційних середовищ і комунікаційних платформ для здійснення терористичних атак або сприяння тероризму. Ці атаки можуть приймати різні форми, як–от поширення пропаганди, викрадення чи маніпулювання даними або порушення критичної інфраструктури. Це також можна назвати актом несанкціонованих атак і створення загроз проти комп'ютерів, мереж і даних, які вони зберігають і поширюють (Theohary & Rollins, 2015). Для

досягнення політичної чи соціальної мети це робиться шляхом залякування чи погроз уряду чи його громадянам. Кібератаки високої інтенсивності також можуть спричинити насильство проти людей або майна або, принаймні, завдати достатньої шкоди, щоб викликати страх. У більшості випадків кібертероризм може призвести до смерті або фізичної шкоди, вибуху, авіакатастрофи, забруднення води або великих економічних чи політичних втрат. Якщо це має великий ефект, кібертероризм може бути здійснений проти основної інфраструктури. Не потрібно повідомляти про атаки, які заважають непотрібним службам або просто заважають. Кібертероризм – це навмисне використання кіберпотужностей, часто недержавними суб'єктами, з першочерговою метою викликати масовий страх, паніку чи збурення серед населення, уряду чи організації. Акти кібертероризму зазвичай включають політично, ідеологічно чи соціально вмотивовані атаки, спрямовані на критичну інфраструктуру, завдають значної шкоди або становлять серйозну загрозу національній безпеці. Те, що відрізняє кібертероризм від інших кібератак, таких як кіберзлочинність або хакерство, полягає в явному намірі розпалювати терор або дестабілізувати суспільства, часто з метою досягнення політичних чи ідеологічних цілей, а не чисто фінансової вигоди чи досягнення соціальних чи етичних цілей. Кібертероризм прагне створити страх, хаос і недовіру в більших масштабах, часто з потенціалом реальної шкоди або руйнування.

– Кібератаки з боку держав (State–sponsored attacks):

Приклад: Ворожі держави фінансують та координують кібератаки на ОКІ з метою саботажу, розвідки або дезінформації. Це можуть бути складні атаки, що включають впровадження шкідливого програмного забезпечення, виведення з ладу систем управління тощо.

Загрози

Під час її виступу у «Department of Justice Criminal Division's Cybersecurity Roundtable on 'The Evolving Cyber Threat Landscape'» заступник генерального прокурора США Ліза Монако заявила, що межа між кіберзлочинців і суб'єктів національної держави розмито: «[держави та кримінальні групи] утворюють

альянси зручності, альянси можливостей а іноді й задумані альянси з акторами національної держави».7

Вісімдесят шість відсотків респондентів вважають, що це дуже ймовірно стали мішенню злочинної організації, яка діяла від імені а національна держава. Судячи з результатів нашого опитування[29], банки, енергетика, оборона, і охорона здоров'я є одними з головних цілей нападу національних держав.

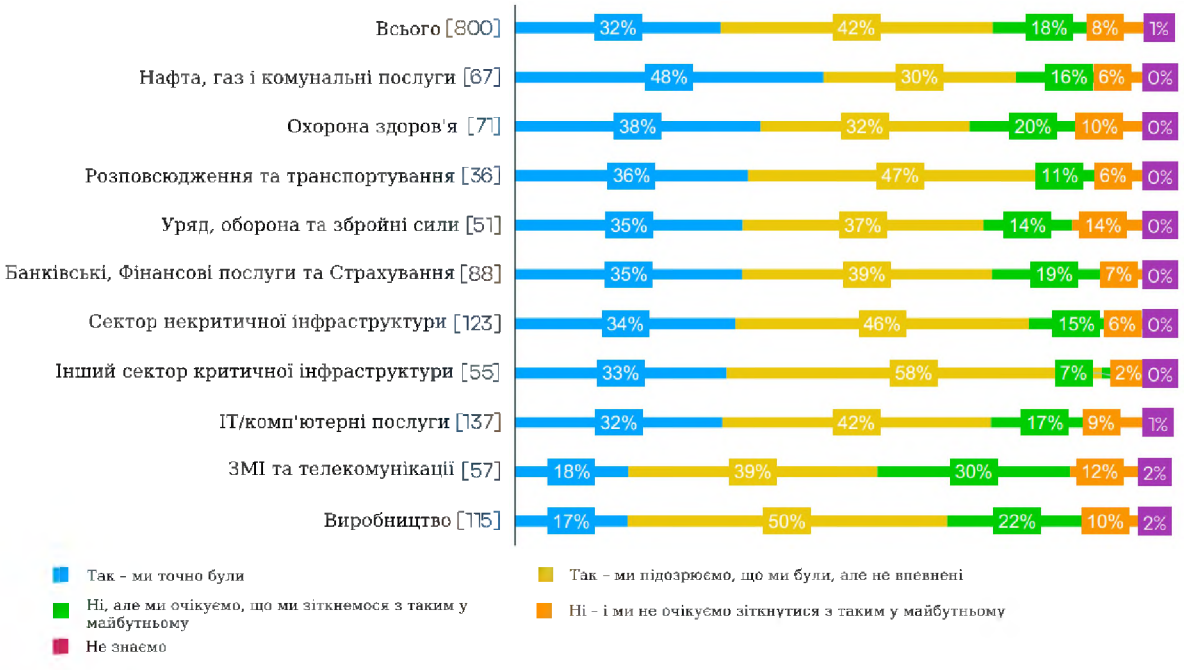

Рисунок 2.5 – Результати опитування: «Чи вважаєте ви, що ваша організація була об’єктом кібератаки національної держави протягом останніх 18 місяців?»

Заходи для протидії зовнішнім загрозам:

– Міжмережеві екрани та системи запобігання вторгнень (Firewalls and Intrusion Prevention Systems – IPS):

Використання сучасних міжмережевих екранів та IPS, таких як «Cisco», для захисту мережі від несанкціонованого доступу та виявлення шкідливої активності, можна назвати самим правильним рішенням для забезпечення найкращого рівня безпеки.

Брандмауери «Cisco» [30] забезпечують розширений брандмауер із збереженням стану та функціональність концентратора VPN в одному пристрої. Крім того, деякі моделі пропонують модуль інтегрованої системи запобігання вторгненням (IPS) або інтегрований модуль безпеки та контролю вмісту (CSC).

Платформи брандмауера «Cisco» включають багато розширених функцій, таких як кілька контекстів безпеки (подібно до віртуалізованих брандмауерів), прозорий (Рівень 2) брандмауер або маршрутизований (Рівень 3) брандмауер, розширені механізми перевірки, IP Security (IPsec) VPN, SSL VPN, і безклієнтська підтримка SSL VPN.

Брандмауери «Cisco» захищають сегменти мережі від несанкціонованого доступу з боку користувачів або зловмисників, а також забезпечують дотримання політик і правил безпеки.

Під час обговорення мереж, підключених до брандмауера, зовнішня мережа зазвичай визначається як розташована перед брандмауером (незахищена область), тоді як внутрішня мережа захищена (за замовчуванням) і знаходиться за брандмауером – довірена зона та демілітаризована зона (сегмент мережі, що містить загальнодоступні сервіси та відокремлює їх від приватних), перебуваючи за брандмауером, дозволяє обмежений доступ зовнішнім (зовнішнім) і внутрішнім (внутрішнім) користувачам. Оскільки «Cisco ASA» дозволяє адміністраторам та інженерам налаштовувати багато інтерфейсів із різними політиками безпеки, ці терміни/назви інтерфейсів використовуються лише в загальному сенсі.

Є ключові деталі, які визначають брандмауер як брандмауер, а не як пристрій пересилання Рівня 3. Брандмауер «Cisco» виконує численні внутрішні функції для забезпечення безпеки середовища. Ці функції включають, але не обмежуються ними:

- Державна перевірка
- Перевірка протоколу рівня 2–7 (видимість протоколу програми)
- Функції нормалізатора TCP
- Обмеження підключення

Це ключові функції, які відрізняють брандмауер Cisco від стандартного пристрою рівня 3.

- Розширений моніторинг та аналіз загроз

Впровадження систем моніторингу та аналізу, що використовують методи машинного навчання для виявлення аномальної активності та потенційних загроз у реальному часі.

Технологія ШІ [31] зробила революцію в галузі кібербезпеки, надаючи численні переваги, які покращують виявлення загроз і реагування на них. Однією з ключових переваг є здатність систем ШІ безперервно аналізувати величезні обсяги даних у режимі реального часу. Це дає змогу ідентифікувати шаблони та аномалії, які можуть свідчити про кібератаку чи потенційне порушення безпеки.

Ще однією перевагою є швидкість, з якою ШІ може виявляти загрози. Традиційні заходи безпеки часто покладаються на ручний аналіз, який займає багато часу та може призвести до помилок людини. Однак за допомогою ШІ алгоритми можуть швидко сканувати масивні набори даних і миттєво позначати будь–яку підозрілу активність.

Крім того, системи на базі штучного інтелекту мають здатність адаптуватися до нових загроз і вчитися на них. Оскільки хакери постійно вдосконалюють свою тактику, для заходів кібербезпеки вкрай важливо бути на крок попереду. Використовуючи алгоритми машинного навчання, ШІ може постійно оновлювати свою базу знань і покращувати свою здатність виявляти нові загрози.

Також, ШІ забезпечує автоматизацію процесів кібербезпеки. Повторювані завдання, такі як моніторинг журналів або реагування на інциденти, можна автоматизувати за допомогою інтелектуальних алгоритмів, що звільняє дорогоцінний час для спеціалістів із безпеки, щоб зосередитися на більш складних питаннях.

Використовуючи можливості обробки природної мови, штучний інтелект може аналізувати письмовий вміст, наприклад електронні листи або журнали чату, на наявність ознак спроб фішингу або зловмисних намірів. Це допомагає організаціям завчасно визначати потенційні ризики, перш ніж вони призведуть до порушення.

І останнє, але не менш важливе: використання штучного інтелекту в кібербезпеці забезпечує підвищену точність і точність під час виявлення загроз.

Машини не схильні до втоми чи відволікань, як люди; вони послідовно застосовують заздалегідь визначені правила без упередженості чи помилок недогляду.

Рисунок 2.6 – Переваги впровадження ШІ в кібербезпеку

– Шифрування та захист даних (Encryption and Data Protection):

Використання методів шифрування для захисту даних як під час передавання, так і при зберіганні, що ускладнює їхнє перехоплення та використання зловмисниками.

Шифрування даних [32] діє як критично важливий захисний засіб у сфері кібербезпеки. Це додає додатковий рівень захисту, гарантуючи, що навіть якщо зловмиснику вдасться отримати доступ до даних, він не зможе прочитати або використати їх без ключа дешифрування. Крім того, шифрування запобігає витоку даних під час передачі, оскільки зашифровані дані марні для тих, хто їх перехоплює без належного ключа дешифрування.

Уявіть, що ви надсилаєте конфіденційний електронний лист із конфіденційною фінансовою інформацією. Без шифрування будь–хто зі зловмисними намірами може перехопити та прочитати електронну пошту, що

потенційно може призвести до крадіжки особистих даних або фінансових втрат. Однак у разі застосування шифрування електронний лист перетворюється на набір символів, який не має сенсу без ключа розшифровки. Це гарантує, що лише призначений одержувач зможе прочитати та зрозуміти вміст електронного листа.

Окрім захисту даних від зовнішніх загроз, шифрування даних також відіграє вирішальну роль у пом'якшенні внутрішніх загроз. Співробітники або особи, які мають авторизований доступ до конфіденційної інформації, можуть становити загрозу безпеці даних. Шифрування гарантує, що навіть якщо інсайдер спробує зловживати або викрасти дані, він не зможе розібратися в них без ключа дешифрування.

– Впровадження антивірусного ПЗ

Більшість зовнішніх загроз, вірусів і фішингових листів, є дуже серйозною проблемою для об'єктів ОКІ. Одним з самих ефективних заходів з безпеки від такого роду загроз, є використання антивірусного програмного забезпечення. Антивіруси допомагають виявити, заблокувати і видалити шкідливе ПЗ, яке могло бути використане для компрометації системи.

Вибір антивірусного програмного забезпечення з високими рейтингами ефективності виявлення та усунення загроз.

Використання антивірусів, таких як Bitdefender, Avast Buiseness або ESET Protect Advanced, які регулярно займають провідні позиції у рейтингах незалежних лабораторій, таких як AV–TEST і AV–Comparatives [33].

Рисунок 2.5 – Найкраще антивірусне ПЗ Windows для бізнес–користувачів

Висновок

Зовнішні загрози становлять серйозну небезпеку для об'єктів критичної інфраструктури через свою різноманітність та непередбачуваність. Ефективна протидія цим загрозам вимагає комплексного підходу, що включає технічні, організаційні та міжнародні заходи. Систематичне впровадження таких заходів допоможе забезпечити надійний захист критичних інфраструктур від зовнішніх атак.

2.3.Існуючі системи захисту та їх ефективність. Приклади покращення системи захисту ОКІ

Ефективний захист інформації на ОКІ, вимагає використання різноманітних систем і технологій, що забезпечують безпеку інформації та запобігають виникненню загроз. В цьому підрозділі буде розглянуто основні типи існуючих систем захисту, їхні функції та оцінку їх ефективності.

Основні системи захисту:

SIEM–системи (Security Information and Event Management):

Security Information & Event Management (SIEM) – це структура безпеки для збору, моніторингу, кореляції та аналізу даних журналу та інформації про події з різних джерел у IT–інфраструктурі організації. Це стосується мереж, серверів, програм, кінцевих точок і пристроїв безпеки, призначених для виявлення потенційних загроз безпеці та вчасного вжиття заходів для зменшення ризиків.

Нариклад можна використовувати такі системи як:

- Splunk;
- IBM QRadar;
- ArcSight.

Оцінка ефективності: SIEM–системи ефективні для виявлення складних та цілеспрямованих атак завдяки можливості кореляції подій та автоматизованого реагування. Проте, їхня ефективність залежить від налаштування правил кореляції та рівня підготовки персоналу.

Системи виявлення та запобігання вторгнень (IDS/IPS):

Системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS) Cisco є одними з багатьох систем, які використовуються як частина підходу до захисту мережі від зловмисного трафіку. Забезпечують виявлення та запобігання спробам несанціонованого доступу до мережевих ресурсів та інформації, шляхом аналізу трафіку та виявлення підозрілої активності

Приклад:

- Snort (IDS);
- Cisco Firepower (IPS).

Оцінка ефективності: IDS/IPS ефективні для виявлення відомих атак та швидкого реагування на них, але можуть бути менш ефективними проти нових або змінених атак, які не входять до їхніх баз даних сигнатур.

Системи ідентифікації та управління доступом (IAM):

Управління ідентифікацією та доступом (IAM) – це безпека та бізнес–дисципліна, яка включає численні технології та бізнес–процеси, щоб допомогти потрібним людям або машинам отримати доступ до потрібних активів у потрібний час із потрібних причин, утримуючи при цьому несанкціонований доступ і шахрайство. IAM–системи забезпечують керування доступом до інформаційних ресурсів на основі ролей та політик, включаючи ідентифікацію користувачів, автентифікацію та авторизацію.

Приклад:

- Okta;
- Microsoft Azure Active Directory.

Оцінка ефективності: IAM–системи ефективні для забезпечення контролю доступу та захисту інформації від несанкціонованого доступу. Завдяки IAM–системам, дуеж зменшується ризик внутрішніх загроз завдяки чіткому розмежуванню прав доступу.

Засоби аудиту безпеки:

Опис: Засоби аудиту безпеки включають інструменти та методи для проведення регулярних перевірок систем безпеки, виявлення вразливостей та оцінки відповідності політикам безпеки. Наприклад, «Nessus» – програма для

автоматичного пошуку відомих вад в захисті інформаційних систем. Nessus є одним з багатьох сканерів вразливостей, які використовуються під час оцінок вразливостей і тестування на проникнення, включаючи шкідливі атаки.

Вона здатна виявити найбільш часто зустрічаються види вразливостей, наприклад:

Наявність вразливих версій служб або доменів Помилки в конфігурації (наприклад, відсутність необхідності авторизації на SMTP–сервері) *Наявність паролів за замовчуванням, порожніх, або слабких паролів

Програма має клієнт–серверну архітектуру, що сильно розширює можливості сканування.

Оцінка ефективності: Засоби аудиту безпеки ефективні для виявлення поточних вразливостей та оцінки стану безпеки систем. Регулярні аудити допомагають забезпечити відповідність стандартам та найкращим практикам.

Шлюзи веб–безпеки (Security Web Gateways):

Опис: Шлюзи веб–безпеки забезпечують контроль доступу до Інтернету, фільтрацію контенту та захист від веб–загроз, включаючи шкідливі веб–сайти та фішинг–атаки.

Захищений веб–шлюз (SWG) – це продукт кібербезпеки, який захищає дані компанії та забезпечує дотримання правил безпеки. SWG працюють між співробітниками компанії та Інтернетом. Подібно до водяного фільтра, який видаляє з води небезпечні домішки, щоб її можна було пити, SWG фільтрують небезпечний вміст із веб–трафіку, щоб зупинити кіберзагрози та витоки даних. Вони також блокують ризиковану або неавторизовану поведінку користувачів.

Усі продукти SWG містять такі технології:

- Фільтрування URL–адрес
- Виявлення та блокування шкідливих програм
- Контроль додатків

SWG можуть також включати запобігання втраті даних (DLP), фільтрацію вмісту та інші фільтри Інтернет–трафіку.

Приклад:

– Zscaler;

– Symantec Web Security Service.

Оцінка ефективності: Шлюзи веб–безпеки ефективні для захисту користувачів від веб–загроз та забезпечення контролю за використанням Інтернету. Вони знижують ризик потрапляння шкідливого програмного забезпечення через веб–браузери.

Висновок

Кожна з систем захисту перерахованих вище, має свої плюси і мінуси, але усі з них відіграють критичну роль у забезпеченні безпеки інформації на ОКІ. Ефективність кожної з систем залежить від її правильного впровадження та постійного регулярного оновлення і вдосконалення. Комплексний підхід до захисту інформації, що заключається в використанні кількох систем одночасно, дозволяє значно підвищити рівень безпеки та знизити ризики.

2.4.Розробка та обґрунтування рекомендацій щодо впровадження нових методів і засобів захисту

Під час розробки рекомендацій, щодо впровадження покращених заходів безпеки інформації, важливо враховувати особливі потреби організації пов'язані з сектором її роботи та рівнем критичності. Для організайцій першого рівню критичності та з паливно–енергетичного сектору, як, наприклад, підприємства ДТЕК, дуже важливим є забезпечення високого рівня захисту та гнучкі налаштування систем доступу і безпеки. Для організацій другого рівня критичності, все ще важливо забезпечення високого рівня захисту безпеки, але все ж таки деякі параметри необов'язкові, та можуть бути вимкнуті або не встановлені.

2.4.1. Рекомендації для організацій щодо захисту від внутрішніх і зовнішніх загроз

В таблиці 2.1 та 2.2, зазначені узагальнені рекомендації щодо розглянутих методів захисту інформації, які були досліджені та детально проаналізовані в цьому розділі. В залежності від категорії критичності, можна знехтувати тим чи іншим методом критичності, або навпаки більш посилено захистити ОКІ від загроз розглянутих у роботі.

Таблиця 2.1 – Рекомендовані методи захисту інформації від внутрішніх загроз

		Рекомендовані методи захисту інформації			
		Моніторинг та аудит	Навчання та тренінг	Контроль доступу	Управління привілеями
Категорія критичності	I	Критично важливо	Критично важливо	Обов’язково	Обов’язково
	II	Обов’язково	Обов’язково	Так	Так
	III	Так	Так	Так	Обов’язково
	IV	–	Так	–	Так

Таблиця 2.2 – Рекомендовані методи захисту інформації від зовнішніх загроз

		Рекомендовані методи захисту інформації				
		Firewall	IDS і IPS	ШІ моніторинг та аудит	Шифрування даних	Антивірусне ПЗ
Категорія критичності	I	Критично важливо	Критично важливо	Обов'язково	Критично важливо	Критично важливо
	II	Критично важливо	Обов'зково	За необхідності	Критично важливо	Критично важливо
	III	Критично важливо	Обов'зково	Так	Обов'зково	Обов'зково
	IV	Обов'зково	Так	Так	Обов'зково	Обов'зково

2.5.Висновки

У цьому розділі було проаналізовано та розглянуто різні способи та засоби захисту безпеки інформації на ОКІ. Основною метою таких заходів є підвищення рівня захищеності від внутрішніх і зовнішніх загроз, що особливо важливо в умовах воєнного стану.

Під час аналізу були представлені кілька перспективних технологій які вже активно використовуються країнами на заході, та після тестувань можуть бути успішно інтегровані в існуючі системи безпеки на об'єктах КІ. Одним з ключових аспектів, стала можливість впровадження методів штучного інтелекту. Завдяки цим мтеодам, стає можлива автоматична ідентифікація потенційних загроз, через аналіз великих обсягів даних у реальному часі.

Ці технології та методи, не тільки підвищують рівень захисту інформації, але й дають можливість швидко адаптуватися до нових загроз. Важливо, що ефективність впровадження таких заходів, значно залежить від їх комплексного застосування та регулярного оновлення. Тільки постійний моніторинг, оцінка ефективності та своєчасне вдосконалення заходів безпеки можуть забезпечити надійний захист інформації на ОКІ в умовах сучасних кіберзагроз та воєнного стану.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Метою розрахунків є економічне обґрунтування доцільності проведення дослідження заходів безпеки інформації на ОКІ. Необхідно визначити розмір капітальних та експлуатаційних витрат на дослідження, можливі збитки у випадку втрати конфіденційної інформації компанії.

3.1. Розрахунок капітальних витрат

Визначення трудомісткості розробки політики безпеки інформації. Для того щоб розрахувати витрати на аналіз даних алгоритмів шифрування, скористуємось формулою 3.1, вказаною нижче:

$$t = t_{\text{тз}} + t_{\text{в}} + t_a + t_{\text{вз}} + t_{\text{озб}} + t_{\text{овр}} + t_{\text{д}}, \text{годин}, \quad (3.1)$$

де $t_{\text{тз}}$ – тривалість складання технічного завдання на розробку політики безпеки інформації складає 16 год;

$t_{\text{в}}$ – тривалість розробки концепції безпеки інформації у організації складає 12 год;

$t_{\text{а}}$ – тривалість процесу аналізу ризиків та загроз складає 48 год;

$t_{\text{вз}}$ – тривалість визначення вимог до заходів, методів та засобів захисту 8 год;

$t_{\text{озб}}$ – тривалість вибору основних рішень з забезпечення безпеки інформації 12 год;

$t_{\text{овр}}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації 6 годин;

$t_{\text{д}}$ – тривалість документального оформлення політики безпеки 8 годин.

$$t = 16 + 12 + 48 + 8 + 12 + 6 + 8 = 110 \text{ годин}$$

3.2. Розрахунки витрат на дослідження та впровадження політик безпеки інформації

Розрахунки приведені нижче, у формулі 3.2, включають в себе заробітну плату спеціаліста з інформаційної безпеки $З_{\text{зп}}$ і вартості витрат машинного часу.

$$К_{\text{рп}} = З_{\text{зп}} + З_{\text{мч}}. \quad (3.2)$$

$$К_{\text{рп}} = 18920 + 119{,}93 = 19039{,}93 \text{ грн}$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{зп} = t + З_{іб}, грн, \quad (3.3)$$

$$З_{зп} = 110 * 172 = 18920 \text{ грн}$$

t – загальна тривалість розробки політики безпеки.

$З_{іб}$ – середньогодинна заробітня плата спеціаліста грн/годину; $З_{іб}$=172 грн.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t + С_{мч}, грн, \quad (3.4)$$

$$З_{мч} = 110 + 9,93 = 119,93 грн,$$

t – трудомісткість дослідження політик безпеки.

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година

$$С_{мч} = P * t_{нал} * C_е + \frac{Ф_{зал} * Н_а}{F_p} + \frac{К_{лпз} * Н_{апз}}{F_p}, грн, \quad (3.5)$$

$$С_{мч} = 0,7 * 2 * 4,32 + \frac{4780 * 0,8}{1920} + \frac{5199 * 0,7}{1920} = 9,93 \text{ грн}$$

де P– встановлена потужність ПК, кВт, 0,7 кВт;

$t_{нал}$ – кількість задіяних робочих станцій при досліджені, 2;

$С_е$ – тариф на електричну енергію, грн/кВт–година, 4,32 грн/кВт–година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн, 40 грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці; $Н_а$ – 0,8;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;$Н_{апз}$ – 0,7;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.; $К_{лпз}$ – 5399 грн;

$F_р$ – річний фонд робочого часу (за 40–годинного робочого тижня $F_р$ = 1920).

Враховуючи відмінності запропонованих рекомендацій для кожного з типів організацій, важливо врахувати їх при розрахунках капітальних витрат. Для розрахунку вартості впровадження методів захисту інформаційної безпеки на ОКІ,

кількість працівників була прийнята за 100. В таблиці 3.1 вказані рекомендоване ПЗ, методи захисту інформації та вартість їх впровадження для обраної організації.

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{рп} + К_{аз} + К_{навч} + К_{кн}, \text{ грн}, \quad (3.6)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн (зовнішні консультанти не були залучені);

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн (для виконання роботи було використано пакет Microsoft Office – 5199 грн; Adobe Photoshop – 2800 грн;)

$К_{пз}$ – вартість створення основного і додаткового програмного забезпечення, тис. грн (під час виконання кваліфікаційної роботи, не було проведено розробки основного і додаткового ПЗ);

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн (під час роботи над кваліфікаційною роботою, було придбано: оперативна пам'ять для покращення продуктивності – Kingston Fury DDR4–3200 вартістю 3999грн; для безпечного збереження прогресу, було придбано джерело безперебійного живлення APC Easy UPS 700VA IEC – 4999 грн);

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн (відсутні);

$К_{н}$– витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн (відсутні).

$$К = 7999 + 8998 = 16997 \text{ грн}$$

3.3. Розрахунок річних експлуатаційних витрат

До щорічних витрат на рекомендовані методи захисту інформації можна віднести методи, що впроваджуються на умовах регулярної підписки. Нижче приведено таблицю 3.1, в якій наведено розглянуті в роботі методи захисту інформації та їх фіксована або річна вартість, використовуючи які, і буде розраховано річні експлуатаційні витрати.

Таблиця 3.1 – Вартість методів захисту інформації

Методи захисту інформації	Фіксована вартість, грн	Щорічні витрати, грн
Моніторинг та Аудит від «ACTIVTRAK»	–	9 202,56
Навчання та підвищення обізнаності, SANS Security Awareness	344087,07	–
Okta Privileged Access	–	6 538,66
IDS/IPS системи MetaFlows Network IDS IPS	–	403 620,80
Антивірусне ПЗ Avast Ultimate Business Security	–	148 200

Для розрахунку річних експлуатаційних витрат потрібно скористатись формулою:

$$C = C_{\text{в}} + C_{\text{к}} + C_{\text{ак}}, \text{тис. грн} \quad (3.7)$$

$C_{\text{в}}$ – вартість Upgrade–відновлення й модернізації системи (не було проведено);

$C_{\text{к}}$ – витрати на керування системою в цілому;

$C_{\text{ак}}$ – витрати, викликані активністю користувачів системи інформаційної безпеки (не було проведено).

$$C_{\text{к}} = C_{\text{н}} + C_{\text{а}} + C_{\text{з}} + C_{\text{ел}} + C_{\text{тос}}, \text{грн} \quad (3.8)$$

де $C_{\text{н}}$ – витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації тощо (Сн – 344087,07 грн).

$C_{\text{з}}$ – річний фонд заробітної плати інженерно–технічного персоналу, що обслуговує систему інформаційної безпеки ($C_{\text{З}}$ – 990720 грн);

$C_{\text{ел}}$ – вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($C_{\text{ел}}$ – 5806,08 грн);

$C_{\text{тос}}$ – Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки;

$С_{ел}$ – визначається за формулою:

$$C_{ел} = P * F * Ц_е \text{ , грн} \quad (3.9)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

$Ц_е$ – тариф на електроенергію, грн/кВт·годин.

$$C_{ел} = 0{,}7 * 1920 * 4{,}32 = 5806{,}08 \text{ , грн}$$

$С_з$ – визначається за формулою:

$$C_з = З_{осн} + З_{дод} \text{ , грн} \quad (3.10)$$

Станом на 2024 рік, середня заробітна плата спеціаліста з інформаційної безпеки становить 172 грн на годину з урахуванням основної і додаткової заробітної плати, а також відрахування на соціальні потреби. Для обслуговування систем безпеки інформації на 1 об'єкті КІ вистачить трьох спеціалістів спеціалістів, отже:

$$C_з = 172 * 176 * 12 * 3 = 1089792 \text{ , грн}$$

Річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ) і дорівнює:

$$C_а = \frac{16997 - 4000}{5} = 2599{,}40 \text{ грн}$$

Використовуючи формулу (3.8) та дані з таблиці 3.1, обчислюємо витрати на керування системою інформаційної безпеки $С_к$:

$$C_к = 344087 + 2599{,}40 + 1089792 + 5806{,}08 + 16997 = 1459281{,}48 \text{ грн}$$

Використовуючи формулу (3.7) обчислюємо річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки:

$$C = 1459{,}3 \text{ тис. грн}$$

3.4. Оцінка величини збитку

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб.;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.;

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих вузлів або сегментів корпоративної мережі;

N – середнє число атак на рік.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V, \tag{3.11}$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

$$П_п = \frac{\sum З_с}{F} * t_п, \tag{3.12}$$

$$П_п = \frac{90816}{176} * 6 = 3096 \text{ грн},$$

де F – місячний фонд робочого часу (при 40–а годинному робочому тижні становить 176 ч).

Витрати На відновлення працездатності корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \quad (3.13)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі,

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с}{F} * t_{ви}, \quad (3.14)$$

$$П_{ви} = \frac{90816}{176} * 3 = 1548 \text{ грн}$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$, і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_с}{F} * t_в, \quad (3.15)$$

$$П_{пв} = \frac{18000}{176} * 3 = 306{,}81 \text{ грн}$$

Тому, використовуючи формулу 3.13, можемо продовжити розрахунки:

$$П_в = 1548 + 306{,}81 + 10000 = 11854{,}81 \text{ грн}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{F_Г} * (t_п + t_в + t_{ви}), \quad (3.16)$$

$$V = \frac{428\,495\,000}{2080} * (6 + 3 + 3) = 2472086{,}54 \text{ грн}$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5–ти денний робочий тиждень, 8–ми годинний робочий день) становить близько 2080 ч.

Отже згідно формули 3.11, упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = 3096 + 11854{,}81 + 2472086{,}54 = 2487037{,}35 \text{ грн}$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації буде складати:

$$\text{В} = \sum_{\text{і}} \sum_{n} U. \quad (3.17)$$

$$\text{В} = 1 * 5 * 2487037{,}35 = 12435186{,}75 \text{ грн}$$

3.5. Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$\text{Е} = B * R - C, \quad (3.18)$$

де В – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн(12435186,75 грн);

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці(під час воєнного стану імовірність становить 50%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн(1459281,48 грн).

$$\text{Е} = 12435186{,}75 * 0{,}5 - 1459281{,}48 = 4758311{,}90 \text{ грн}$$

3.6. Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу наступних показників:

– сукупна вартість володіння (ТСО);

– коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

– термін окупності капітальних інвестицій T_o.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K}, \text{частка одиниці} \quad (3.19)$$

Де: Е – загальний ефект від впровадження системи інформаційної безпеки (розділ 3.5 методичних вказівок, формула 3.17), тис. грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

$$ROSI = \frac{4758311,90}{1456682,08} = 3,3$$

Якщо організація здійснює фінансування капітальних інвестицій у систему інформаційної безпеки за рахунок позикових коштів, тобто за рахунок банківського кредиту, то в якості бажаного значення $E_н$ варто приймати величину плати за кредит (кредитної ставки) $N_{кр}$.

Якщо розрахункове значення коефіцієнта повернення інвестицій перевищує банківську кредитну ставку з урахуванням інфляції, проект визнається доцільним:

$$ROSI > (N_{кр} + N_{інф})/100 \quad (3.20)$$

де $N_{кр}$ – банківська кредитна ставка, %;

$N_{інф}$ – річний рівень інфляції, %.

$$3,3 > (17,5 + 100,6)/100$$

$$3,3 > 1,181$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_o = \frac{K}{E} = \frac{1}{ROSI}, \text{років} \quad (3.21)$$

$$T_o = \frac{1}{3,3} = 0,3 \text{ років}$$

3.7. Висновки

В економічній частині дипломного проекту обґрунтовано доцільність розробки нових політик безпеци, розраховано його собівартість (1459281,48 грн, розрахована загальна сума збитків при відсутності запровадження 12435186,75 грн).

При виконанні економічної частини, зробивши всі необхідні розрахунки, встановлено, що технологія розробки програмного продукту відповідає оптимальному рівню витрат, і, в кінцевому підсумку, розроблений продукт є економічно доцільним та конкурентоспроможним для впровадження в технічному відділі підприємства та окупається замовником за менше ніж за пів року.

ВИСНОВКИ

Отже, у кваліфікаційній роботі було розглянуто об’єкти критичної інфраструктури, способи та методи їх категоризації, а також було розглянуто можливі загрози безпеці об’єктам критичної інфраструктури та інформації на них під час війни, які було проведено атаки у зарубіжних країнах та які наслідки вони мали.

Також було розглянуто більше детально загрози які існують саме для комп’ютерних систем на ОКІ та які покращення потрібно впровадити для захисту інформації на них. Було розраховано вартість введення новітніх систем захисту інформації, та проведено розрахунок доцільності їх введення.

Забезпечення інформаційної безпеки на ОКІ під час воєнного стану вимагає комплексного підходу, що включає технічні, організаційні та правові заходи. Лише за умови їх належної реалізації можна гарантувати стабільне та безпечне функціонування критично важливих об'єктів. Ці заходи були ретельно розглянуті в спеціальному розділі, а в економічному розділі було розраховано їх доцільність. Також було пораховано вартість їх введення та фінансові втрати у випадку атаки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Об'єкти критичної інфраструктури України: все, що варто знати [Електронний ресурс] URL: https://www.kyivpost.com/uk/post/28283 (дата звернення 04.06.2024);

2. Про критичну інфраструктуру : Закон України від 01.01.2024 р. №1882–IX. URL: https://zakon.rada.gov.ua/laws/show/1882–20#Text (дата звернення: 03.06.2024).

3. Деякі питання об’єктів критичної інфраструктури : Постанова від 20.01.2024 р. №1109–2020–п. URL: https://zakon.rada.gov.ua/laws/show/1109–2020–%D0%BF#Text (дата звернення: 04.06.2024).

4. Об'єкти критичної інфраструктури: детальний аналіз та відповіді на поширені питання [Електронний ресурс] URL: https://smarttender.biz/blog/view/ob–yekti–kritichnoyi–infrastrukturi–detalniy–analiz–ta–vidpovidi–na–poshireni–pitannya/ (дата звернення 03.06.2024);

5. Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури : Наказ від 15.01.2021 р. №v0023519–21. URL: https://zakon.rada.gov.ua/laws/show/1882–20#Text (дата звернення: 06.06.2024).

6. Кібероперації рф: нові цілі, інструменти та групи. Аналітика хакерських атак проти України за 2 півріччя 2023 року [Електронний ресурс] URL: https://cip.gov.ua/ua/news/kiberoperaciyi–rf–novi–cili–instrumenti–ta–grupi–analitika–khakerskikh–atak–proti–ukrayini–za–2–pivrichchya–2023–roku (дата звернення 15.06.2024);

7. Російські ракетні удари пошкодили всі великі електростанції України, крім АЕС – «Укренерго» [Електронний ресурс] URL: https://forbes.ua/news/rosiyski–raketni–udari–poshkodili–vsi–veliki–elektrostantsii–ukraini–krim–aes–ukrenergo–22112022–9947 (дата звернення 08.06.2024);

8. Через пошкодження магістрального газопроводу знизили тиск газу в мережі Донеччини [Електронний ресурс] URL: https://www.epravda.com.ua/news/2022/12/28/695529/ (дата звернення 08.06.2024);

9. Випробовування холерою: як олігархи, президент–вигнанець і блокада знищують Ємен [Електронний ресурс/стаття] URL: https://hromadske.ua/posts/vyprobovuvannia–kholeroiu–iak–oliharkhy–prezydent–vyhnanets–i–blokada–znyshchuiut–yemen (дата звернення 08.06.2024);

10. Що таке саботаж та як себе не викрити [Електронний ресурс] URL: https://sprotyv.mod.gov.ua/shho–take–sabotazh–ta–yak–sebe–ne–vykryty/ (дата звернення 08.06.2024);

11. Що таке кібератака? [Електронний ресурс] URL: https://www.microsoft.com/uk–ua/security/business/security–101/what–is–a–cyberattack (дата звернення 08.06.2024);

12. Огляд кібератак на об'єкти критичної інфраструктури [Електронний ресурс] URL: https://web.archive.org/web/20200507145857id_/https://www.emodel.org.ua/images/em/41–6/%D0%BA%D0%BE%D0%BC%D0%B0%D1%80%D0%BE%D0%B2.pdf (дата звернення 08.06.2024);

13. Що таке багатофакторна автентифікація (MFA)? [Електронний ресурс] URL: https://cloud.smart–it.com/news–post/what–is–mfa/ (дата звернення 11.06.2024);

14. Захоплюючий світ шифрування – розгляд типів, алгоритмів та їх застосувань [Електронний ресурс] URL: https://hackyourmom.com/pryvatnist/zahoplyuyuchyj–svit–shyfruvannya–rozglyad–typiv–algorytmiv–ta–yih–zastosuvan/ (дата звернення 11.06.2024);

15. Дослідження систем виявлення та попередження вторгнень у комп'ютерні мережі [Електронний ресурс] URL: https://core.ac.uk/download/pdf/81587611.pdf (дата звернення 11.06.2024);

16. Підприємства ДТЕК [Електронний ресурс] URL: https://join.dtek.com/ua/pidprijemstva/ (дата звернення 16.06.2024);

17. Як розподіляється доступна електроенергія між всіма споживачами Дніпропетровщини, – пояснює ДТЕК Дніпровські електромережі [Електронний ресурс] URL: https://www.dtek–dnem.com.ua/ua/news/yak–rozpodilyayetsya–

dostupna–elektroenergiya–mizh–vsima–spozhivachami–dnipropetrovshchini–poyasnyuye–dtek–dniprovski–elektromerezhi (дата звернення 16.06.2024);

18. Енергетики створили віртуальний сервер для цифрового газовидобутку [Електронний ресурс] URL: https://ua–energy.org/uk/posts/enerhetyky–stvoryly–virtualnyi–server–dlia–tsyfrovoho–hazovydobutku (дата звернення 18.06.2024);

19. Наставления по кибербезопасности (ISO/IEC 27032:2012): изложение стандарта ISO/IEC 27032:2012 "Информационные технологии.– Методы обеспечения безопасности – Наставления по кибербезопасности" Мохор Владимир Владимирович. [Електронний ресурс] URL: https://zenodo.org/records/3866468 (дата звернення 16.06.2024);

20. NIST SP 800–39, Managing Information Security Risk: Organization, Mission, and Information System View [Електронний ресурс] URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800–39.pdf (дата звернення 18.06.2024);

21. According to Gurucul Survey One in Four Workers Would Steal Company Information to Secure Job at Competing Firm [Електронний ресурс] URL: https://www.businesswire.com/news/home/20190827005135/en/Gurucul–Survey–Workers–Steal–Company–Information–Secure (дата звернення 19.06.2024);

22. The Cost of Human Error in Cybersecurity [Електронний ресурс] URL: https://www.linkedin.com/pulse/cost–human–error–cybersecurity–michael–robinette?trk=article–ssr–frontend–pulse_more–articles_related–content–card (дата звернення 19.06.2024);

23. What is Privileged Access Management (PAM)? [Електронний ресурс] URL: https://www.cyberark.com/what–is/privileged–access–management/#:~:text=PAM%20refers%20to%20a%20comprehensive,across%20an%20enterprise%20IT%20environment (дата звернення 19.06.2024);

24. INSIDER THREAT INDICATORS IN USER ACTIVITY MONITORING [Електронний ресурс] URL: https://www.cdse.edu/Portals/124/Documents/jobaids/insider/Insider–Threat–Indicators–in–UAM.pdf (дата звернення 19.06.2024);

25. SANS Security Awareness [Електронний ресурс] URL: https://www.cisecurity.org/services/cis–cybermarket/sans–security–awareness (дата звернення 19.06.2024);

26. Role–Based Access Controls [Електронний ресурс] URL: https://csrc.nist.gov/files/pubs/conference/1992/10/13/rolebased–access–controls/final/docs/ferraiolo–kuhn–92.pdf (дата звернення 19.06.2024);

27. What you need to know about NIST 800–53, least privilege, and PAM [Електронний ресурс] URL: https://delinea.com/blog/nist–800–53–security–privacy–privileged–access (дата звернення 19.06.2024);

28. Volatile Geopolitics Shake the Trends of the 2022 Cybersecurity Threat Landscape [Електронний ресурс] URL: https://www.enisa.europa.eu/news/volatile–geopolitics–shake–the–trends–of–the–2022–cybersecurity–threat–landscape (дата звернення 19.06.2024);

29. Cyberterrorism as a global threat: a review on repercussions and countermeasures [Електронний ресурс] URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10803091/ (дата звернення 19.06.2024);

30. Cisco Firewall Best Practices [Електронний ресурс] URL: https://sec.cloudapps.cisco.com/security/center/resources/firewall_best_practices#2 (дата звернення 20.06.2024);

31. The Role of Artificial Intelligence in Cybersecurity: Enhancing Threat Detection and Response [Електронний ресурс] URL: https://medium.com/@analyticsemergingindia/the–role–of–artificial–intelligence–in–cybersecurity–enhancing–threat–detection–and–response–6ca0b202be72 (дата звернення 20.06.2024);

32. Essential Data Encryption Best Practices [Електронний ресурс] URL: https://www.kiteworks.com/secure–file–sharing/secure–file–sharing–essential–data–encryption–best–practices/#The_Role_of_Data_Encryption_in_Cybersecurity (дата звернення 20.06.2024);

33. The best Windows antivirus software for business users [Електронний ресурс] URL: https://www.av–test.org/en/antivirus/business–windows–client/ (дата звернення 21.06.2024);

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	20	
6	А4	2 Розділ	28	
7	А4	3 Розділ	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	5	
10	А4	Додаток А	1	
11	А4	Додаток Б	13	
12	А4	Додаток В	6	
13	А4	Додаток Г	1	
14	А4	Додаток Ґ	1	
15	А4	Додаток Д	1	

ДОДАТОК Б. Визначення рівня негативного впливу на надання послуг під час категоризації секторальних ОКІ

ВИЗНАЧЕННЯ РІВНЯ
негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури (секторальні критерії)

Сектор/під сектор		Фактор негативного впливу в секторі/підсекторі	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка $\sum PK_i$
1.	Послуги, що надаються підсектором електроенергетики та підсектором ядерної енергетики	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення електропостачання	для більш як 145 000 жителів або для споживачів I категорії на території більш як однієї області або на території не менш як трьох міст обласного значення	для більш як 30 000 жителів або для споживачів II категорії на території однієї області або на території більш як одного району міста – обласного центру, або на всій території одного міста обласного значення	для більш як 2000 жителів	для менш як 2000 жителів	
			час відновлення функціонування у штатному режимі не може перевищувати 6 годин	час відновлення функціонування у штатному режимі може становити від 6 до 24 годин	час відновлення функціонування у штатному режимі може становити від однієї до трьох діб	час відновлення функціонування у штатному режимі може становить більше трьох діб	
2.	Послуги, що надаються підсектором енергетичного машинобудування	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення виробництва та надання послуг з ремонту силових трансформаторів та реакторів	для більш як 145 000 жителів на території більш як однієї області або не менш як трьох міст обласного значення	для більш як 30 000 жителів на території області або більш як одного району міста – обласного центру, або на всій території одного міста обласного значення	для більш як 6000 жителів	не застосовується	

3.	Послуги, що надаються підсектором вугільно–промислового комплексу та підсектором торфодобування	знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури призведе до припинення видобутку вугілля або торфу, постачання на об’єкти генерації (теплоелектростанціях та теплоелектроцентралях)	для більш як 30 000 жителів на території однієї області або на території більш як одного району міста – обласного центру, або на всій території одного міста	для більш як 10 000 жителів	для більш як 5000 жителів	для менш як 5000 жителів	
			час відновлення функціонування у штатному режимі не може перевищувати 6 годин	час відновлення функціонування у штатному режимі може становити від 6 до 24 годин	час відновлення функціонування у штатному режимі може становити від однієї до трьох діб	час відновлення функціонування у штатному режимі становить більше трьох діб	
4.	Послуги, що надаються підсектором нафтової промисловості	знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури призведе до зменшення обсягів постачання нафти та нафтопродуктів для споживання на внутрішньому ринку	більш як на 25 відсотків порівняно з аналогічним періодом календарного року чи попереднього календарного місяця	від 12 до 25 відсотків порівняно з аналогічним періодом календарного року чи попереднього календарного місяця	від 7 до 12 відсотків порівняно з аналогічним періодом календарного року чи попереднім календарним місяцем	менш як на 7 відсотків порівняно з аналогічним періодом календарного року чи попереднім календарним місяцем	
5.	Послуги, що надаються підсектором газової промисловості	знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури призведе до припинення постачання газу	для більш як 145 000 жителів або для споживачів з безперервною подачею газу на території більш як однієї області або на території не менш як трьох міст обласного значення	для більш як 20 000 жителів на території однієї області або на території більш як одного району міста – обласного центру, або на всій території одного міста обласного значення	для більш як 5000 жителів	для менш як 5000 жителів	

			час відновлення функціонування у штатному режимі не може перевищувати 6 годин	час відновлення функціонування у штатному режимі може становити від 6 до 24 годин	час відновлення функціонування у штатному режимі від однієї до трьох діб	час відновлення функціонування у штатному режимі може бути більше трьох діб	
6.	Послуги, що надаються інформаційним сектором та сектором цифрових технологій	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення або зменшення обсягу надання основних послуг об'єктом	для більш як 145 000 жителів на території більш як однієї області або на території не менш як трьох міст обласного значення	для більш як 20 000 жителів на території однієї області або на території більш як одного району міста – обласного центру, або на всій території одного міста обласного значення	для більш як 2000 жителів	для менше як 2000 жителів	
			час відновлення функціонування у штатному режимі не може перевищувати 6 годин	час відновлення функціонування у штатному режимі може становити від 6 до 24 годин	час відновлення функціонування у штатному режимі може становити від однієї до трьох діб	час відновлення функціонування у штатному режимі становить більше трьох діб	
7.	Послуги, що надаються підсектором електронних комунікацій	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення або зменшення обсягу надання основних послуг	втрата можливості функціонування елементів електронної комунікаційної мережі або мережевої інфраструктури або інфраструктури центру обробки даних чи обміну трафіком для України або значної її частини	збій, переривання у наданні основних послуг або обмеження доступу користувачам послуг чи сервісів для великих міст чи цілих регіонів	відсутність стабільного з'єднання, переривання сесій, зниження пропускної здатності електронних комунікаційних мереж для операторів або частини користувачів	не застосовується	
8.	Послуги з постачання теплової енергії та гарячої води	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення	для більш як 145 000 жителів або на території більш як однієї області, або не менш як трьох міст обласного значення	для більш як 30000 жителів або на території більш як одного району міста – обласного центру, або на всій території одного міста обласного значення	для більш як 2000 жителів	для менш як 2000 жителів	

		постачання теплової енергії та/або гарячої води буде перервано (під час опалювального сезону)					
			час відновлення функціонування у штатному режимі не може перевищувати 24 годин	час відновлення функціонування у штатному режимі може становити від доби до трьох діб	час відновлення функціонування у штатному режимі може становити від трьох діб	не застосовується	
9.	Послуги з централізованого питного водопостачання	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення централізованого водопостачання	для більш як 145 000 жителів або на території більш як однієї області, або не менш як трьох міст обласного значення	для більш як 30000 жителів або стаціонарним лікувальним закладам, будинкам соціальної допомоги, установам, що надають послуги освіти на території області або більш як одного району міста – обласного центру, або на всій території одного міста обласного значення	для більш як 2000 жителів	для менш як 2000 жителів	
			час відновлення функціонування у штатному режимі не може перевищувати 24 годин (час кризової ситуації не може перевищувати 24 годин)	час відновлення функціонування у штатному режимі може становити від доби до трьох діб (час кризової ситуації може становити від доби до трьох діб)	час відновлення функціонування у штатному режимі може становити від доби до трьох діб (час кризової ситуації може становити від доби до трьох діб)	не застосовується	
10.	Послуги з централізованого водовідведення	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення централізованого водовідведення	для більш як 145 000 жителів або на території обласного центру, або не менш як трьох міст обласного значення	для більш як 30 000 жителів або на території одного міського району обласного центру, або на всій території одного міста обласного значення	для більш як 2000 жителів	для менше як 2000 жителів	

		та очищення стічних вод					
			час відновлення функціонування у штатному режимі не може перевищувати 24 годин (час кризової ситуації не може перевищувати 24 годин)	час відновлення функціонування у штатному режимі може становити від доби до трьох діб (час кризової ситуації може становити від доби до трьох діб)	час відновлення функціонування у штатному режимі може становити від трьох діб (час кризової ситуації може становити від доби до трьох діб)	не застосовується	
11.	Послуги з управління побутовими відходами	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення збору, зберігання, безпечної переробки (утилізації) побутових відходів	для більш як 145 000 жителів або на території обласного центру, або не менш як трьох міст обласного значення	для більш як 30 000 жителів або на території одного міського району обласного центру, або на всій території одного міста обласного значення	не застосовується	не застосовується	
12.	Послуги, що надаються підсектором авіаційного транспорту	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури	неможливість надання послуг з перевезення пасажирів та вантажів авіаційним транспортом (хоча б одним із стратегічно важливих аеропортів України) протягом більш як 24 години без можливості організації альтернативного способу надання послуг	неможливість надання послуг з перевезення пасажирів та вантажів авіаційним транспортом (хоча б одним із стратегічно важливих аеропортів України) протягом більш як 24 години з можливістю організації альтернативного способу надання послуги	припинення повітряного руху на час відновлення штатного режиму функціонування	не застосовується	
13.	Послуги, що надаються підсектором автомобільного транспорту	знищення, пошкодження або порушення функціонування об'єкта	блокування (припинення) дорожнього руху на мостах, шляхопроводах, міжнародних та національних	блокування (припинення) дорожнього руху на мостах, шляхопроводах, міжнародних та національних дорогах	блокування (припинення) дорожнього руху на мостах, шляхопроводах,	блокування (припинення) дорожнього руху на мостах, шляхопроводах,	

		критичної інфраструктури	дорогах більш як на 24 години за відсутності обхідного шляху або відсутність можливості його відновлення протягом не більш як 24 години	не більш як на 24 години за відсутності обхідного шляху	регіональних дорогах протягом не більш як на 48 годин за відсутності обхідного шляху або відсутності можливості його відновлення протягом не більш як 48 годин	регіональних дорогах протягом не більш як на 48 годин за відсутності обхідного шляху	
14.	Послуги, що надаються підсектором залізничного транспорту	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури	припинення залізничного руху на залізничних магістральних лініях I (I–П, I–ПС) та II категорій (ДБН В.2.3–19–2018) за часом, що перевищує 24 години, за відсутності можливості забезпечення руху обхідною залізничною лінією або суміжною колією, а також через штучні споруди (мости, шляхопроводи, віадуки, тунелі), розташовані на залізничній магістральній лінії від кордонів з країнами Європейського Союзу до найближчої вузлової станції, та інші мости повною довжиною понад 1000 метрів	припинення залізничного руху на залізничних магістральних лініях III категорії (ДБН В.2.3–19–2018) за часом, що перевищує 24 години, за відсутності можливості забезпечення руху обхідною залізничною лінією або через суміжною колією, а також через штучні споруди (мости, шляхопроводи, віадуки, тунелі), розташовані на залізничній магістральній лінії від кордонів з країнами Європейського Союзу до найближчої вузлової станції, та інші мости повною довжиною понад 1000 метрів	припинення залізничного руху на залізничних магістральних лініях IV категорії (ДБН В.2.3–19–2018) за часом, що перевищує 24 години, за відсутності можливості забезпечення руху обхідною залізничною лінією або суміжною колією, а також через штучні споруди (мости, шляхопроводи, віадуки, тунелі), які розташовані на залізничній магістральній лінії від кордонів з країнами Європейського Союзу до найближчої вузлової станції, та інші мости повною довжиною понад 1000 метрів	припинення залізничного руху на залізничних магістральних лініях V категорії (ДБН В.2.3–19–2018) за часом, що перевищує 24 години, за відсутності можливості забезпечення руху обхідною залізничною лінією або суміжною колією, а також через штучні споруди (мости, шляхопроводи, віадуки, тунелі), які розташовані на залізничній магістральній лінії від кордонів з країнами Європейського союзу до найближчої вузлової станції, та інші мости повною довжиною понад 1000 метрів	

15.	Послуги, що надаються підсектором морського та внутрішнього водного транспорту	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури	припинення надання морських послуг у морських портах більш як на 72 години (Правила надання послуг у морських портах України, затверджені наказом Мінінфраструктури від 5 червня 2013 р. № 348)	час припинення надання морських послуг у морських портах може становити від 24 до 72 годин	час припинення надання морських послуг у морських портах може становити не більше як 24 години	не застосовується	
16.	Послуги, що надаються підсектором метрополітену	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури	припинення надання послуг з перевезення пасажирів більш як на 45 відсотків загальних пасажирських перевезень міста або на території, що охоплює більше 50 відсотків районів міста	припинення надання послуг більш як 15 відсотків загальних пасажирських перевезень міста або на території, що охоплює більше 25 відсотків районів міста	припинення надання послуг більш як 5 відсотків загальних пасажирських перевезень міста або на території, що охоплює більше 10 відсотків районів міста	припинення надання послуг до 5 відсотків загальних пасажирських перевезень міста або на території, що охоплює до 10 відсотків районів міста	
17.	Послуги із збереження функціонування міждержавних та місцевих пунктів пропуску через державний кордон для автомобільного сполучення	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	блокування (припинення) роботи міжнародних, міждержавних та місцевих пунктів пропуску через державний кордон для автомобільного сполучення більш як на 24 години за відсутності можливості відновлення його роботи протягом не більш як 24 години	блокування (припинення) роботи міжнародних та міждержавних пунктів пропуску через державний кордон для автомобільного сполучення не більш як на 24 години за відсутності альтернативного способу надання послуг	блокування (припинення) роботи місцевих пунктів пропуску через державний кордон для автомобільного сполучення протягом не більш як на 48 годин за відсутності можливості відновлення його роботи протягом не більш як 48 годин	блокування (припинення) роботи місцевих пунктів пропуску через державний кордон для автомобільного сполучення протягом не більш як на 48 годин за відсутності альтернативного способу надання послуг	
18.	Послуги, що надаються підсектором поштового зв'язку	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення	для більш як 145 000 жителів на території більш як однієї області або більш як трьох міст обласного значення	для більш як 20 000 жителів на території області або більше одного району міста – обласного центру, або на всій території одного міста обласного значення	для більш як 6000 жителів	для менш як 6000 жителів	

		надання послуг поштового зв'язку					
19.	Послуги, що надаються сектором промисловості	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	для більш як 100 000 жителів на території більш як однієї області або не менш як трьох міст обласного значення	для більш як 30 000 жителів на території області або більш як одного району міста – обласного центру, або на всій території одного міста обласного значення	для більш як 6000 жителів	для менш як 6000 жителів	
20.	Послуги, що надаються фінансовим сектором	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	для більш як 100 000 клієнтів	для більш як 50 000 клієнтів	для більш як 10 000 клієнтів	не застосовується	
21.	Послуги, що надаються сектором харчової промисловості та агропромислового комплексу, сектором охорони навколишнього природного середовища, сектором охорони здоров'я, сектором цивільного захисту населення та територій, сектором соціального захисту	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	для більш як 145 000 жителів на території більш як однієї області або не менш як трьох міст обласного значення	для більш як 30 000 жителів на території області або більш як одного району міста – обласного центру, або на всій території одного міста обласного значення	для більш як 6000 жителів	для менш як 6000 жителів	
22.	Послуги, що надаються сектором державного матеріального резерву (зберігання	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури	для більш як 145 000 жителів або для споживачів I категорії на території більш як однієї області або не менш як	для більш як 30 000 жителів або для споживачів II категорії на території області або більш як одного району міста – обласного центру, або на всій	для більш як 2000 жителів	для менш як 2000 жителів	

	запасів державного матеріального резерву)	призведе до ненадання об'єктом основних послуг	трьох міст обласного значення	території одного міста обласного значення			
			час відновлення функціонування у штатному режимі не може перевищувати 6 годин	час відновлення функціонування у штатному режимі може становити від 6 до 24 годин	час відновлення функціонування у штатному режимі може становити від однієї до трьох діб	час відновлення функціонування у штатному режимі може становити більше трьох діб	
23.	Послуги, що надаються сектором громадської безпеки	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	для більш як 145 000 жителів або на території більш як однієї області, або не менш як трьох міст обласного значення	для більш як 30000 жителів або на території більш як одного району міста обласного центру, або на всій території одного міста обласного значення	для більш як 2000 абонентів	для менше як 2000 абонентів	
24.	Послуги, що надаються підсектором екстреної допомоги населенню за єдиним телефонним номером 112	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення оперативного цілодобове невідкладного реагування на екстрені комунікації, їх оброблення, зберігання та передача інформації про такі комунікації для надання допомоги населенню за єдиним телефонним номером 112	для більш як 145 000 жителів або на території більш як однієї області, або не менш як трьох міст обласного значення	для більш як 30000 жителів або на території більш як одного району міста обласного центру, або на всій території одного міста обласного значення	для більш як 2000 абонентів	для менше як 2000 абонентів	
25.	Послуги, що надаються сектором правосуддя	знищення, пошкодження або порушення функціонування об'єкта	на всій території України	на території однієї або декількох областей	на території району області або району міста	не застосовується	

		критичної інфраструктури					
			припинення надання послуг за відсутності можливості невідкладно організувати альтернативний спосіб їх надання			припинення надання послуг за відсутності можливості невідкладно організувати альтернативний спосіб їх надання	
26.	Послуги, що надаються сектором “Вибори та референдуми”	знищення, пошкодження або порушення функціонування об’єкта інфраструктури призведе до неможливості організації підготовки та проведення виборів чи референдуму відповідно до вимог закону	неможливість здійснення суб’єктами виборчого процесу/ процесу референдуму виборчих процедур/ процедур референдуму на загальнодержавних виборах/всеукраїнському референдумі без можливості організації альтернативного способу здійснення відповідних процедур у межах встановленого законодавством строку	неможливість здійснення суб’єктами виборчого процесу/процесу референдуму виборчих процедур/процедур референдуму на місцевих виборах/місцевому референдумі без можливості організації альтернативного способу здійснення відповідних процедур у межах встановленого законодавством строку	відсутність можливості здійснення суб’єктами виборчого процесу/процесу референдуму виборчих процедур/ процедур референдуму за наявності можливості організації альтернативного способу здійснення відповідних процедур у межах встановленого законодавством строку	неможливість здійснення суб’єктами виборчого процесу/процесу референдуму виборчих процедур/ процедур референдуму, що не впливає на надання основної послуги	
			час відновлення функціонування у штатному режимі не може перевищувати встановлений законодавством строк здійснення відповідних процедур на загальнодержавних виборах/ всеукраїнському референдумі без можливості організації альтернативного способу їх здійснення	час відновлення функціонування у штатному режимі не може перевищувати встановлений законодавством строк здійснення відповідних процедур на місцевих виборах/місцевому референдумі без можливості організації альтернативного способу їх здійснення	час відновлення функціонування у штатному режимі не може перевищувати встановлений законодавством строк здійснення відповідних виборчих процедур/ процедур референдуму за наявності можливості організації	час відновлення функціонування у штатному режимі може перевищувати встановлений законодавством строк здійснення відповідних виборчих процедур/ процедур референдуму	

					альтернативного способу їх здійснення		
27.	Послуги оборони	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	для жителів на території більш як двох – трьох областей або не менш як однієї області	для жителів на території більш як однієї області або не менш як трьох міст обласного значення	для жителів на території області або більш як одного району міста – обласного центру, або на всій території одного міста обласного значення	для жителів більш як одного району області або на всій території одного міста районного значення	
28.	Послуги, що надаються підсектором зберігання ракет, боєприпасів та вибухових речовин	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	для забезпечення боєприпасами військових частин на території більш як трьох областей	для забезпечення боєприпасами військових частин на території двох областей або не менше однієї області	для забезпечення боєприпасами військових частин на території однієї області або не менше трьох районів області	для забезпечення боєприпасами військових частин двох – трьох районів області	
29.	Послуги, що надаються сектором виконання кримінальних покарань, тримання під вартою та утримання військовополонених	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	для більш як 145 000 жителів на території більш як однієї області або не менш як трьох міст обласного значення	для більш як 20 000 жителів на території області або більше одного району міста – обласного центру, або на всій території одного міста обласного значення	для більш як 5000 жителів	для менш як 5000 жителів	
			припинення надання послуг з виконання кримінальних покарань, попереднього ув'язнення та тримання військовополонених більш як на 72 години	припинення надання послуг з виконання кримінальних покарань, попереднього ув'язнення та тримання військовополонених може становити від 48 до 72 годин	припинення надання послуг з виконання кримінальних покарань, попереднього ув'язнення та тримання військовополонених може становити від 24 до 48 годин	припинення надання послуг з виконання кримінальних покарань, попереднього ув'язнення та тримання військовополонених може становити не більше 24 годин	
30.	Послуги, що надаються сектором ринків	знищення, пошкодження або порушення функціонування	для більш як 25 000 учасників ринку капіталу та їх клієнтів	для більш як 10 000 учасників ринку капіталу та їх клієнтів	для більш як 5 000 учасників ринку	не застосовується	

	капіталу та організованих товарних ринків	об'єкта критичної інфраструктури призведе до припинення або порушення надання об'єктом основних послуг			капіталу та їх клієнтів		
			час відновлення функціонування у штатному режимі не може перевищувати 6 годин	час відновлення функціонування у штатному режимі може становити від 6 до 24 годин	час відновлення функціонування у штатному режимі може становити від однієї до трьох діб	час відновлення функціонування у штатному режимі може становити більше трьох діб	
31.	Послуги, що надаються сектором наукових досліджень та розробок	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення виконання досліджень, у тому числі тих, що виконуються для сектору безпеки та оборони з міжнародними договорами, укладеними від імені України	неможливість надання послуг з проведення наукових досліджень, які здійснюються за замовленням держави для важливих секторів економіки та безпеки, а також за міжнародними договорами, укладеними від імені України	втрата унікального наукового обладнання, яке забезпечує надання послуг з проведення наукових досліджень, які здійснюються за замовленням держави для важливих секторів економіки та безпеки, а також за міжнародними договорами, укладеними від імені України	неможливість надання послуг з проведення наукових досліджень співвиконавцем наукових досліджень, які здійснюються за замовленням держави для важливих секторів економіки та безпеки, а також за міжнародними договорами, укладеними від імені України	не застосовується	
32.	Послуги, що надаються сектором державної влади та місцевого самоврядування	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	для жителів на території всієї країни	для жителів на території однієї області	для жителів на території територіальної громади	для жителів на території одного району міста обласного значення	
33.	Послуги (сервіси) кіберзахисту	у разі знищення або пошкодження, порушення	припинення надання послуг, які надаються на національному	припинення надання послуг, які надаються на регіональному/міжрегіо	наслідком є припинення надання послуг, які	припинення надання послуг операторам	

		сталого функціонування об’єкта критичної інфраструктури	рівні (двом і більше) центральним органам виконавчої влади, державним органам, Національному банку та об’єктам критичної інфраструктури I категорії критичності	нальному, галузевому/міжгалузевому рівні центральному органу виконавчої влади, визначеним відповідальними за забезпечення формування та реалізацію державної політики у сфері захисту критичної інфраструктури в окремому секторі, центральному органу виконавчої влади, двом та більше місцевим держадміністраціям (військово–цивільним адміністраціям – у разі створення), двом та більше місцевим органам виконавчої влади, об’єктам критичної інфраструктури II категорії критичності	надаються на місцевому рівні органу виконавчої влади (військово–цивільній адміністрації – у разі створення), органу місцевого самоврядування, об’єктам критичної інфраструктури III, IV категорії критичності	критичної інфраструктури на об’єктовому рівні

ДОДАТОК В. Визначення рівня негативного впливу на надання послуг під час категоризації міжсекторальних ОКІ

ВИЗНАЧЕННЯ РІВНЯ
негативного впливу у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури (міжсекторальні критерії)

Негативний вплив		Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бал)	Рівень негативного впливу: незначні наслідки (1 бал)	Рівень негативного впливу: надто малий (0 балів)	Оцінка РКі
I. Соціальна значущість об'єкта критичної інфраструктури							
1.	Заподіяння шкоди життю та здоров'ю людей	Кількість населення, що може постраждати					
		небезпека для життя або здоров'я більш як 75 000 людей	небезпека для життя та здоров'я більш як 5000 людей	небезпека для життя або здоров'я більш як 50 людей	небезпека для життя або здоров'я менш як 50 людей	не критично	$РК_1$ =
		Географічний масштаб					
		небезпека для життя та здоров'я мешканців на території однієї або більш як однієї області, або на території трьох та більше міст обласного значення	небезпека для життя та здоров'я мешканців на території однієї області або міського району міста обласного центру, або на всій території одного міста обласного значення	небезпека для життя та здоров'я для людей на території об'єкта та для мешканців, що проживають у безпосередній близькості до розміщення об'єкта	небезпека для життя та здоров'я людей на території об'єкта	не критично	$РК_2$ =
2.	Заподіяння шкоди навколишньому природному середовищу	Економічні втрати					
		нанесені збитки більш як 30 млн. гривень	нанесені збитки більш як 18 млн. гривень	нанесені збитки більш як 2 млн. гривень	нанесені збитки менш як на 2 млн. гривень	не критично	$РК_3$ =

		Географічний масштаб					
		шкідливий вплив розповсюджується на територію більш як однієї області або на території не менш як трьох міст обласного значення	шкідливий вплив розповсюджуєтьс я на територію однієї області або на територію більш як одного міста обласного значення	шкідливий вплив розповсюджує ться на територію одного міста обласного значення	шкідливий вплив розповсюджує ться на територію об'єкта інфраструктур и	не критично	$РК_4$ =
		Час					
		шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом більш як одного року	шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом від півроку до одного року	шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом від одного місяця до півроку	шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом одного місяця	не критично	$РК_5$ =
II. Суспільна значущість об'єкта критичної інфраструктури							
3.	Припинення або порушення функціонування державних органів	припинення або порушення функціонуванн я Верховної Ради України, Кабінету Міністрів України, Конституційног о Суду України, Верховного Суду, а також Офісу Президента України, Ради національної безпеки та оборони України	припинення або порушення функціонування центральних органів виконавчої влади та облдержадміністр ацій	припинення або порушення роботи районних держадміністр ацій, територіальни х органів центральних органів виконавчої влади	припинення або порушення роботи органів місцевого самоврядуван ня	не критично	$РК_6$ =

4.	Негативний вплив на довіру людей до державних інституцій	матиме значний вплив				не критично	$РК_7$ =
5.	Шкода інтересам інших держав – партнерів України	так, принаймні двом країнам або порушення умов міжнародного договору, укладеного від імені України	так, принаймні одній країні або порушення умов міжнародного договору, укладеного від імені Уряду України	можливі негативні наслідки для інших держав, але їх вплив навряд чи буде значним	держави не постраждають або не має місце порушення умов міжнародного договору, укладеного від імені міністерства, іншого центрального органу виконавчої влади, державного органу	не критично	$РК_8$ =
III. Економічна значущість об’єкта критичної інфраструктури							
6.	Заподіяння збитків оператору критичної інфраструктури (у відсотках прогнозованого обсягу річного доходу за всіма видами діяльності)	більш як 15 відсотків	від 10 до 15 відсотків	від 5 до 10 відсотків	менш як 5 відсотків	не критично	$РК_9$ =
7.	Заподіяння збитків державному бюджету (зниження прибутків бюджету у відсотках	більш як 0,1 відсотка	від 0,1 до 0,05 відсотка	від 0,05 до 0,01 відсотка	менш як 0,01 відсотка	не критично	$РК_{10}$ =

	прогнозованого річного прибутку бюджету)						
8.	Заподіяння збитків місцевим бюджетам (зниження прибутків бюджету у відсотках прогнозованого річного прибутку бюджету)	більш як 0,1 відсотка	від 0,1 до 0,05 відсотка	від 0,05 до 0,01 відсотка	менш як 0,01 відсотка	не критично	$РК_{11}$ =
IV. Взаємозв'язок між об'єктами критичної інфраструктури							
9.	Негативний вплив на безперервне та стійке функціонування іншого об'єкта інфраструктури, що забезпечує надання таких самих основних послуг	матиме негативний вплив (якщо так, вкажіть який)				не критично	$РК_{12}$ =
10.	Негативний вплив на безперервне та стійке функціонування іншого об'єкта інфраструктури, що надає інші основні послуги	матиме негативний вплив (якщо так, вкажіть який)				не критично	$РК_{13}$ =
V. Значущість об'єкта критичної інфраструктури для забезпечення національної безпеки та обороноздатності країни							

11.	Припинення або порушення (невиконання встановлених показників) функціонування пунктів управління (ситуаційного центру), що оцінюється в рівні (значущості) пункту управління або ситуаційного центру	припинення або порушення функціонування пунктів управління Верховного Головнокомандувача Збройних Сил, Головнокомандувача Збройних Сил, Начальника Генерального штабу Збройних Сил або ситуаційного центру Офісу Президента України, Кабінету Міністрів України, Ради національної безпеки та оборони України	припинення або порушення функціонування пунктів управління або ситуаційного центру центральних органів виконавчої влади, інших державних органів, органів державного управління, юрисдикція яких поширюється на всю територію України, пунктів управління Сухопутних військ, Повітряних Сил, Військово–Морських Сил, десантно–штурмових військ, сил спеціальних операцій, Національної гвардії, Держприкордонслужби	припинення або порушення функціонування обласної державної адміністрації, ситуаційних центрів	припинення або порушення функціонування територіальних органів центральних органів виконавчої влади	не критично	$РК_{14}$ =
12.	Припинення або порушення виробництва товарів, виконання робіт та надання послуг оборонного призначення, які є предметом оборонних закупівель, для забезпеченн	Зниження обсягів продукції (робіт, послуг) в заданий період часу (у відсотках)					
		більш як 15 відсотків	від 10 до 15 відсотків	від 5 до 10 відсотків	менше як 5 відсотків	не критично	$РК_{15}$ =
		Збільшення часу виготовлення продукції (робіт, послуг) із заданим обсягом (відсотків встановленого часу на виготовлення продукції)					
		більш як 40 відсотків	від 10 до 40 відсотків	від 5 до 10 відсотків	менш як 5 відсотків	не критично	$РК_{16}$ =

	я потреб сектору безпеки і оборони, а також інших товарів, робіт і послуг для гарантовано го забезпечення потреб безпеки і оборони						
Усього $\sum РК_i$							

ДОДАТОК Г. Перелік документів на оптичному носії

Пояснювальна записка_Музичук.docx

Презентація.pptx

ДОДАТОК Г. Відгуки керівників розділів

Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 90 б. («відмінно»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Д. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:

студента групи 125–20–3
Музичук Денис Сергійович

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 95 сторінках та містить 9 рисунка, 3 таблиці, 33 джерел та 6 додатка.

Представлена кваліфікаційна робота на ступінь бакалавра присвячена розробці методів та засобів захисту інформації на об'єктах критичної інфраструктури. По справжній день, технології захисту інформації в інформаційних системах на об'єктах критичної інфраструктури все ще потребують модернізації та покращення рівня захисту. Позитивними рисами дипломної роботи є системність та послідовність викладення матеріалу. З огляду на це, робота бакалавра характеризується актуальністю та своєчасністю.

Студентом було проведено аналіз та порівняння можливих методів розв'язання поставленої задачі та обрано оптимальний варіант. Крім того, було досліджено існуючі реалізації розв'язання подібних задач. Під час виконання кваліфікаційної роботи рівня бакалавра студент Музичук Д.С. проявив себе грамотним, кваліфікованим спеціалістом здатним приймати самостійно складні технічні рішення. Вважаю, що кваліфікаційна робота заслуговує на оцінку «відмінно», а Музичук Д.С. – присвоєння кваліфікації «бакалавра» з кібербезпеки.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою, відповідає вимогам положення про систему запобігання та виявлення плагіату у Національному технічному університеті «Дніпровська політехніка». Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку 90 б. «відмінно».

Керівник кваліфікаційної роботи доц. Ковальова Ю.В.
Керівник спец. розділу доц. Ковальова Ю.В.