МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра кібербезпеки

«До захисту допущено»

Завідувач кафедри

_____ Володимир ЛЮБЧАК
(підпис) (Ім'я та ПРІЗВИЩЕ)

___ _____ 20__р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавр

зі спеціальності 125 Кібербезпека та захист інформації, освітньо-професійної програми Кібербезпека на тему: Дослідження шляхів забезпечення інформаційної безпеки критичної інфраструктури згідно чинного законодавства України

Здобувачки групи КБ-01 Підлісної Анастасії Андріївни
(шифр групи) (прізвище, ім'я, по батькові)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Анастасія ПІДЛІСНА
(підпис) (Ім'я та ПРІЗВИЩЕ здобувача)

Керівник старший викладач, кандидат фізико-математичних наук,
(посада, науковий ступінь, вчене звання, Ім'я та ПРІЗВИЩЕ)

Віталій КОВАЛЬ _____
(посада, науковий ступінь, вчене звання, Ім'я та ПРІЗВИЩЕ) (підпис)

Суми-2024

Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра кібербезпеки

«Затверджую»
Завідувач кафедри

_____ Володимир ЛЮБЧАК
(підпис)
«___»_____ 20___ р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня бакалавр

зі спеціальності 125 – Кібербезпека, освітньо-професійної програми «Кібербезпека»

здобувачки групи КБ-01 Підлісної Анастасії Андріївни

1.Тема роботи: «Дослідження шляхів забезпечення інформаційної безпеки критичної інфраструктури згідно чинного законодавства України»

затверджено наказом по СумДУ №0212-VI від «04» березня 2024 р.

2. Термін подання студентом роботи: «04» червня 2024 р.

3. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити): важливість об'єктів критичної інфраструктури, огляд методологій інформаційної безпеки енергетичної інфраструктури, розробка рекомендацій стосовно підтримки актуальності апаратного та програмного забезпечення.

5. Дата видачі завдання «____» _____ 20 ___ р.

Завдання прийняв до виконання _____ (підпис)

Керівник _____ (підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання	Примітка
1			
2			
3			
4			
5			

Здобувач вищої освіти _____ Керівник _____

(підпис) (підпис)

Анотація

Кваліфікаційна робота виконана на 54 аркушах та містить 11 таблиць, 1 додаток та 22 джерела.

Об’єкт дослідження: процес забезпечення інформаційної безпеки критичної інфраструктури України.

Мета роботи: огляд чинного законодавства України в сфері захисту критичної інфраструктури, зокрема в енергетичному секторі, та розробка рекомендації реалізації підтримки актуальності апаратного та програмного забезпечення.

Методи дослідження: системний аналіз, метод зіставлення, синтез.

Результати роботи: розроблено рекомендації стосовно підтримки актуальності апаратного та програмного забезпечення відповідно до вимоги чинного законодавства і таким чином розширено документ щодо планових заходів кіберзахисту об’єкту критичної інфраструктури паливно-енергетичного сектору.

Ключові слова: критична інфраструктура, інформаційна безпека, законодавство України, інформаційна система, програмне забезпечення, операційна система, апаратне забезпечення.

Зміст

Перелік скорочень, умовних позначень, термінів

КІ – критична інфраструктура

ОЕС – об’єднана електроенергетична система

НЕК – національна енергетична компанія

СНД – співдружність незалежних держав

АЕС – атомна електростанція

ТЕС – теплова електростанція

ТЕЦ - теплоелектроцентраль

ГЕС – гідроелектростанція

ВДЕ – відновлювані джерела енергії

ОЗП – оперативний запам'ятовуючий пристрій

ПЗ – програмне забезпечення

ОС – операційна система

ЦОД – центр опрацювання даних

АСКУЕ – автоматизована система контролю та обліку енергоресурсів

АСУТП – автоматизована система керування технологічним процесом

СУБД – система управління базами даних

НПЗ – нафтопереробний завод

НАК – національна акціонерна компанія

ВСТУП

Швидке впровадження інформаційних технологій та глобалізація обміну інформацією призвели до тенденції переміщення незаконної діяльності у кіберпростір. У наші дні комп’ютерна злочинність загрожує не лише пересічним громадянам, а й виходить за межі державних кордонів і посягає на національні інтереси. Проблема боротьби з кіберзлочинністю на державному рівні є актуальною внаслідок активного використання інформаційних технологій у всіх сферах життєдіяльності. Однією з таких є функціонування критичної інфраструктури, яка включає такі галузі, як енергетика, транспорт, зв'язок, водопостачання та інші, діяльність яких впливає на безпеку та добробут держави. Наслідки, пов’язані з можливістю атак на ці сектори, є катастрофічними та можуть призвести до дефіциту енергії, збоїв у транспортних системах, зв’язку та доступу до необхідних ресурсів.

В Україні існують загрози, пов’язані з поточною геополітичною ситуацією. Кібератаки на об’єкти критичної інфраструктури можуть використовуватися як тактика гібридної війни, щоб дестабілізувати державу. Це потребує створення надійної системи захисту інформаційних ресурсів.

Питання забезпечення інформаційної безпеки критичної інфраструктури регламентується низкою нормативних актів. Дотримання чинного законодавства є одним із визначальних факторів, який може сприяти встановленню належного рівня захисту інформації для збереження стабільності та безпеки держави. Законодавство держави викладає загальні поняття діяльності із захисту інформації та визначає суб’єкта відповідальності за її здійснення. Законодавча база встановлює вимоги для захисту інформаційних ресурсів та окреслює заходи контролю та відповідальність за невиконання. Також наголошує на створенні та впровадженні ефективних планів і технологій захисту, проведенні професійних

навчань, налагодженні систем реагування на інциденти та співпраці з відповідними організаціями та органами влади.

Предметом дослідження є діяльність критичної інфраструктури енергетично-паливного сектору.

Об'єктом дослідження є процес забезпечення інформаційної безпеки критичної інфраструктури України.

Метою роботи є огляд чинного законодавства України в сфері захисту критичної інфраструктури, зокрема в енергетичному секторі, та розробка рекомендації реалізації підтримки актуальності апаратного та програмного забезпечення.

Тезу з обґрунтуванням необхідності виконання вимог законодавства стосовно захисту об’єктів критичної інфраструктури від кіберзагроз опубліковано у матеріалах Міжнародної наукової конференції молодих учених «IMA::2024», 22-26 квітня 2024 року.

1 ОГЛЯД ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Загальне поняття критичної інфраструктури

У сучасному світі суспільство повністю залежне від послуг, які надають енергетичні, транспортні, телекомунікаційні, водопостачальні та інші інфраструктурні мережі. Якість життя в певній місцевості характеризується доступністю цих послуг. Країни які мають високо розвинені інфраструктурні об'єкти, мають змогу бути сучасними економічними центрами, розвивати та зосереджувати на своїй території фінансові, промислові та інтелектуальні потужності. Вихід з ладу цих систем може призвести до масштабних проблем та великих фінансових втрат. Негативними факторами впливу на об'єкти можуть виступати процеси природного, техногенного та соціально-політичного характеру. Ці загрози несуть небезпеку для функціонування суспільно-важливих об'єктів, а отже забезпечення їх захисту стає серйозним викликом навіть для економічно розвинутих держав. Тому існує необхідність зосередити ресурси на захисті життєво важливих інфраструктурних об'єктів, що обумовлює розвиток та впровадження концепції критичної інфраструктури (КІ) як складової систем забезпечення національної безпеки.

В Україні під поняттям «критична інфраструктура» розуміється переважно енергетична, транспортна, водопостачальна системи. Однак, насправді, цей термін є набагато ширшим. Критична інфраструктура була і залишається головним об'єктом захисту, адже становить першочерговий інтерес кіберзлочинців. Окрім людського фактору, вона також піддається ураженню природного характеру. Тому, надзвичайно важливо зрозуміти визначення, суть і складові указаного поняття для створення ефективної структури інформаційного захисту з можливістю надання належної відповіді кібератакам.

Постанова Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг від 14.03.2018 р. № 309 «Про затвердження Кодексу системи передачі» визначає критичну інфраструктуру як сукупність об'єктів системи передачі або її частини, що входять до складу ОЕС України, та є необхідними для забезпечення життєво важливих для суспільства функцій, охорони здоров'я, безпеки та добробуту населення, виведення з ладу або руйнування яких матиме суттєвий вплив на національну безпеку та оборону, навколишнє природне середовище та може призвести до значних фінансових збитків і людських жертв [16].

Подібне але менше визначення надає Постанова Кабінету Міністрів України від 23 серпня 2016 р. № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави», а саме, критична інфраструктура – сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних фінансових збитків та людських жертв [17].

Найбільш лаконічне визначення надається в Законі України «Про критичну інфраструктуру», критична інфраструктура – сукупність об'єктів критичної інфраструктури [1].

Об'єкти критичної інфраструктури - об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [1]. Вони виконують життєво важливі функції та надають послуги, а саме:

- урядування та надання найважливіших публічних (адміністративних) послуг;
- енергозабезпечення (у тому числі постачання теплової енергії);
- водопостачання та водовідведення;
- продовольче забезпечення;
- охорона здоров’я;
- фармацевтична промисловість;
- виготовлення вакцин, стале функціонування біолабораторій;
- інформаційні послуги;
- електронні комунікації;
- фінансові послуги;
- транспортне забезпечення;
- оборона, державна безпека;
- правопорядок, здійснення правосуддя, тримання під вартою;
- цивільний захист населення та територій, служби порятунку;
- космічна діяльність, космічні технології та послуги;
- хімічна промисловість;
- дослідницька діяльність.

Залежно від надаваних послуг, згідно з Постановою Кабінету Міністрів від 9 жовтня 2020 р. N 1109 «Деякі питання об'єктів критичної інфраструктури» об’єкти критичної інфраструктури розділяються на сектори:

- паливно-енергетичний сектор;
- інформаційний сектор;
- системи життєзабезпечення;
- харчова промисловість та агропромисловий комплекс;

- охорона здоров'я;
- ринки капіталу та організовані товарні ринки;
- транспорт і пошта;
- промисловість;
- цивільний захист населення та територій;
- фінансовий сектор [18].

Щоб визначити необхідні вимоги щодо забезпечення відповідного захисту, об’єкти критичної інфраструктури класифікуються за наступними категоріями критичності:

1) І категорія критичності - особливо важливі об’єкти, які мають життєво важливе значення для країни, мають великий вплив на інші ключові об’єкти інфраструктури та порушення яких спричинить велику національну катастрофу;
2) ІІ категорія критичності – життєво важливі об’єкти, порушення функціонування яких призведе до виникнення значущої для регіону кризової ситуації;
3) ІІІ категорія критичності - важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення;
4) IV категорія критичності - необхідні об’єкти, порушення функціонування яких призведе до виникнення локальної кризової ситуації.

1.2 Паливно-енергетичний сектор

Інфраструктура системи енергозабезпечення є критично важливою для функціонування суспільства, оскільки від її стабільної роботи залежить ефективне функціонування базових галузей промисловості, транспорту та житлово-комунального комплексу.

Енергетична інфраструктура сприяє економічному розвитку. Електроенергія, а також інші види енергії необхідні для роботи промисловості, сільського господарства, транспорту та інших секторів країни. Енергія є передумовою для створення продуктів і послуг, а також для створення та впровадження нових технологій. Стабільне енергопостачання допомагає прогнозувати дії підприємств, розширювати потужності та підвищувати їх конкурентоспроможність на внутрішньому та зовнішньому ринках. Окрім цього, безперервне та стабільне електро- та теплопостачання є ключовим компонентом добробуту населення. Наявність електроенергії сприяє розвитку освіти, культури та медицини, що, у свою чергу, покращує рівень життя людей. Система енергетики також сприяє національній безпеці, забезпечує функціонування військових об’єктів, телекомунікацій, транспорту та іншої інфраструктури, важливої для захисту країни.

В Україні паливно-енергетичний сектор добре розвинений та складається з підсекторів.

Таблиця 1.1 – Відомості про підсектори паливно-енергетичного сектору згідно з Постанова Кабінету Міністрів від 9 жовтня 2020 р. N 1109 «Деякі питання об'єктів критичної інфраструктури»

Уповноважений орган державної влади, відповідальний за сектор (підсектор) критичної інфраструктури	**Сектор**	**Підсектор**	**Тип основної послуги**
Міненерго	Паливно-енергетичний	електроенергетика	виробництво електричної енергії, забезпечення функціонування ринку електричної енергії, розподіл електричної енергії
		нафтова промисловість	видобуток нафти, передача нафти та нафтопродуктів очищення, переробка та обробка нафти, експлуатація нафтопроводів.

Продовження таблиці 1.1

1	2	3	4
		газова промисловість	видобуток газу, переробка та очищення газу, передача (транзит) газу, розподіл газу, експлуатація газотранспортної системи, зберігання природного газу, забезпечення роботи систем зрідження природного газу
		ядерна енергетика	виробництво електричної енергії на атомних станціях, експлуатація атомних станцій, виробництво, переробка та зберігання ядерного палива, поводження з радіоактивними відходами

1.2.1 Електроенергетика

В Україні основою електроенергетики є об’єднана електроенергетична система (ОЕС), яка централізовано постачає електроенергію власним споживачам і зв’язується з енергосистемами сусідніх країн для забезпечення імпорту та експорту електроенергії.

Згідно із Законом України "Про електроенергетику" одним з основних напрямків державної політики в електроенергетиці є збереження цілісності та забезпечення надійного і ефективного функціонування ОЕС України, єдиного диспетчерського (оперативно-технологічного) управління нею. Забезпечення виконання цих функцій в Україні покладено на Державне підприємство НЕК "Укренерго" [2].

НЕК «Укренерго» у своїй виробничій діяльності дотримується наступних стратегій:

- забезпечення надійної передачі електроенергії між електростанціями по електричним мережам напругою понад 220 кВ;
- створення необхідної бази для функціонування міждержавних та магістральних електромереж як невід’ємної частини інфраструктури ринку електроенергії;
- централізація оперативно-технологічного управління об’єднаною енергосистемою;
- забезпечення цілісності енергосистеми країни, запобігання порушень режимів і аварій системного значення, а також ліквідація аварій з найменшими збитками для держави;
- забезпечення надійної паралельної роботи теплових, атомних і гідроелектростанцій та їх взаємодію з енергосистемами країн СНД, Східної та Центральної Європи.

Українська електроенергетика представлена різними типами електростанцій, включаючи атомні, теплові, гідроелектростанції та відновлювальні джерела енергії.

Понад половину електроенергії в Україні виробляють атомні електростанції (АЕС), що робить їх основними виробниками електроенергії в країні. У нашій державі діють чотири атомні електростанції: Південноукраїнська, Хмельницька, Рівненська та Запорізька, яка є найбільшою атомною електростанцією в Європі. Атомні енергетичні установки дуже надійні та ефективні, але через можливість радіаційних аварій вони потребують контролю безпеки.

Вугілля, природний газ і мазут є видами палива, які використовуються на теплових електростанціях (ТЕС) для виробництва електроенергії. Основні ТЕС знаходяться в індустріально розвинених районах, таких як Дніпропетровська, Луганська та Донецька області. Незважаючи на те, що ТЕС достатньо пристосовані для роботи на різних видах палива, вони є основним джерелом викидів забруднюючих речовин, таких як вуглекислий газ та інші забруднювачі повітря.

Гідроелектростанції (ГЕС) для виробництва енергії використовують потенціал річок. Дністровська ГЕС і Дніпровський каскад є двома основними гідроенергетичними об’єктами України. Здатність гідроелектростанцій швидко адаптуватися до коливань попиту на енергію робить гідроенергію надзвичайно важливою для підтримки пікових навантажень і регулювання функціонування енергосистеми.

Останнім часом в Україні зросло використання відновлюваних джерел енергії (ВДЕ) – сонячної та вітрової. Частка ВДЕ у загальному обсязі виробленої електроенергії невпинно зростає завдяки державній підтримці у цій сфері.

1.2.2 Нафтова промисловість

Нафтова промисловість України відіграє важливу роль у економіці країни. Вона забезпечує близько 10% потреб країни у нафті та є одним з основних джерел надходжень до бюджету. Найбільшою нафтовою компанією є «Укрнафта», на її частку припадає близько 90% українського нафтовидобутку.

В Україні діють шість основних нафтопереробних заводів (НПЗ) — Лисичанський, Кременчуцький, Херсонський, Дрогобицький, Одеський, Надвірнянський. Найбільшими з них є Кременчуцький, Лисичанський та Дрогобицький НПЗ. Ці підприємства забезпечують переробку сирої нафти в паливо, мастила та інші нафтопродукти.

Транспортування нафти в Україні здійснюється через розгалужену систему трубопроводів, яка з'єднує основні нафтогазові родовища з нафтопереробними заводами та експортними терміналами. Одним з важливих елементів цієї системи є магістральні нафтопроводи "Дружба" та "Одеса-Броди". Ці нафтопроводи забезпечують транспортування нафти не лише на внутрішньому ринку, але й для експорту в країни Європи.

Важливість захисту нафтової промисловості обумовлена кількома факторами. Перш за все, нафта є одним з основних джерел енергії для України, що використовується для опалення, виробництва електроенергії, роботи транспорту та промислових потреб. Перебої в роботі нафтопереробних заводів, трубопроводів або інших критичних об'єктів можуть призвести до дефіциту енергії, що матиме негативні наслідки для економіки та життєдіяльності населення. Крім того, так як нафтові компанії вносять значну частку прибутку до державного бюджету, то порушення в роботі нафтової галузі можуть призвести до суттєвих фінансових проблем, що негативно позначиться на економічній стабільності країни.

1.2.3 Газова промисловість

Розвідка, видобуток, транспортування, зберігання та переробка природного газу, а також супутнього нафтового газу, що видобувається разом з нафтою, входять до функцій газової промисловості. Природний газ використовується для виробництва електроенергії, тепла та транспорту. Завдяки постійному зростанню значення в енергопостачанні це джерело енергії розвивається найвищими темпами. Він є домінуючим видом палива в енергетичному балансі України, забезпечуючи понад 40% потреб країни в енергії. Незважаючи на те, що він використовується в багатьох галузях промисловості, більшість природного газу використовується в енергетичному секторі, оскільки це паливо, що найменш забруднює навколишнє середовище.

Найбільші запаси природного газу містяться у трьох основних газових басейнах: Дніпровсько-Донецький, Карпатськомий та Причорноморсько-Кримський. Видобуток газу здійснюється як державними, так і приватними компаніями. Найбільшим з них є "Укргазвидобування", дочірня компанія НАК "Нафтогаз України". Вони роблять значний внесок у ВВП країни, створюють велику кількість робочих місць і сприяють зростанню інших секторів економіки. Діяльність газової промисловості безпосередньо впливає на добробут населення, забезпечуючи безперебійну роботу значної кількості виробничих і промислових підприємств. Газові компанії також підтримують розвиток регіональної інфраструктури, місцевої торгівлі та регіональних громад.

Україна має одну з найбільших у світі систем транспортування природного газу, що включає понад 37 тисяч кілометрів газопроводів та кілька підземних сховищ газу, які використовуються для забезпечення стабільного постачання газу в періоди пікового споживання. Такі сховища також відіграють важливу роль у

підтриманні надійності газопостачання та забезпеченні енергетичної безпеки країни.

1.2.4 Ядерна енергетика

Атомна енергетика забезпечує до 60% загального виробництва електроенергії в Україні. Наразі, в Україні діють 4 атомні електростанції (АЕС): Рівненська АЕС, Хмельницька АЕС, Запорізька АЕС, Південноукраїнська АЕС. Найбільшою та найпотужнішою в Європі є Запорізька АЕС з 6 енергоблоками загальною потужністю 6 ГВт.

Використання ядерної енергетики зменшує залежність України від імпорту енергоносіїв. Вона відіграє важливу роль у забезпеченні енергетичних потреб країни, забезпечуючи стабільне та надійне електропостачання для промисловості, житлового сектору та інших життєво важливих сфер.

Атомні електростанції можуть працювати безперервно протягом тривалого часу, забезпечуючи стабільне електропостачання в будь-який час доби та за будь-яких погодних умов. Для підтримки такого режиму функціонування виникає потреба у побудові ефективного захисту від негативного впливу, який може порушити сталу роботу АЕС. Це є не лише питанням у межах однієї держави, але й має важливе значення для міжнародної безпеки та стабільності. Забезпечення безпечної експлуатації АЕС потребує значних інвестицій та постійного контролю.

Наслідки аварії на Чорнобильській АЕС в 1986 році, хоч і спричинили значні зміни в українському ядерному секторі, однак не призвели до повної відмови від нього. Україна вдосконалила свої стандарти безпеки, а також впровадила міжнародні норми та стандарти МАГАТЕ щоб посилити захист ядерних установок.

2 ОГЛЯД МЕТОДОЛОГІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

2.1 Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»

Документ описує загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, які визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури [5].

Надано визначення таким поняттям: критичні бізнес/операційні процеси об'єкта критичної інфраструктури, система інформаційної безпеки, політика інформаційної безпеки.

Окрім загальних вимог в документі міститься додаток, у якому описано перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури, а саме:

- формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки;
- управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;
- ідентифікація та автентифікація користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

- реєстрація подій компонентами об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та їх періодичний аудит;
- забезпечення мережевого захисту компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;
- забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;
- визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури;
- визначення умов використання програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;
- визначення умов розміщення компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури [5].

2.2 Закон України «Про критичну інфраструктуру»

Закон України «Про критичну інфраструктуру» визначає правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки [1].

Закон містить шість розділів:

- Розділ 1. Загальні положення: визначає основні поняття, цілі та завдання закону
- Розділ 2. Основні засади державної політики у сфері захисту критичної інфраструктури: визначає мету, завдання державної політики, основні принципи та рівні управління національною системою захисту
- Розділ 3. Критична інфраструктура України: встановлюються критерії для визначення об'єктів, що підлягають включенню до реєстру критичної інфраструктури, визначаються сектори, категорії критичності.
- Розділ 4. Національна система захисту критичної інфраструктури: визначає обов'язки власників та операторів об'єктів критичної інфраструктури, а також порядок їх взаємодії з органами державної влади для забезпечення належного рівня захисту.
- Розділ 5. Організаційні засади національної системи захисту критичної інфраструктури: описуються вимоги щодо планування заходів захисту, проведення моніторингу та аудиту, а також міжнародного співробітництва.
- Розділ 6. Прикінцеві та перехідні положення: містить положення щодо набрання чинності законом, перехідні положення, а також вносить зміни до інших законодавчих актів у зв'язку з прийняттям цього закону.

2.3 Постанова Кабінету Міністрів України від 11.11.2020 № 1176 «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом»

Цей Порядок визначає організаційні засади проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом [11].

Надано визначення таким поняттям: життєво важливі послуги та функції, кіберстійкість критичної інформаційної інфраструктури, оцінювання стану кіберзахисту, суб'єкт критичної інформаційної інфраструктури, уповноважений орган державної влади, відповідальний за сектор (підсектор) економіки або сферу діяльності.

2.4 Постанови Кабінету Міністрів України від 29 грудня 2021 р. № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту»

Це Положення визначає механізм функціонування організаційно-технічної моделі кіберзахисту [8].

Надано визначення таким поняттям: базисна інфраструктура кіберзахисту, кібергігієна, команди реагування на комп'ютерні надзвичайні події, організаційно-керуюча інфраструктура кіберзахисту, технологічна інфраструктура кіберзахисту, сили кіберзахисту.

Основною метою затвердженого Положення є встановлення комплексного підходу до кіберзахисту, який поєднує організаційні та технічні заходи для забезпечення безпеки інформаційних систем. Положення визначає основні

завдання та обов’язки органів державної влади, підприємств, установ та організацій, що є суб’єктами критичної інформаційної інфраструктури, у сфері кіберзахисту.

2.5 Постанова Кабінету Міністрів України від 23.12.2020 № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки»

Цей Порядок визначає засади функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, які здійснюються щодо об’єктів кіберзахисту, визначених частиною другою статті 4 Закону України “Про основні засади забезпечення кібербезпеки України”. Дія цього Порядку не поширюється на об’єкти критичної інформаційної інфраструктури Міноборони та Збройних Сил в умовах надзвичайного і воєнного стану. [12].

Надано визначення таким поняттям: адміністратор безпеки об’єкта кіберзахисту, адміністратор безпеки системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, галузевий центр з управління кібербезпекою, мережева телеметрія, політика безпеки, система виявлення вразливостей і реагування на кіберінциденти та кібератаки, центр з управління кібербезпекою.

Головною метою постанови є розробка скоординованого та ефективного підходу до виявлення загроз в інформаційних системах і мережах, швидкого реагування на кіберзагрози та кібератаки.

2.6 Постанова Кабінету Міністрів України від 04.04.2023 № 299 «Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі»

Цей Порядок визначає процедури реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі та категорії (рівні) їх критичності [13].

Основною метою постанови є створення системи швидкого та ефективного реагування на кіберінциденти, щоб забезпечити захист інформаційних ресурсів критичної інфраструктури. У документі визначаються конкретні обов'язки та дії, які мають здійснювати суб'єкти у разі виникнення кіберінцидентів.

2.7 Постанова Кабінету Міністрів України від 16.05.2023 № 497 «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»

Цей Порядок визначає механізм здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж [14].

Дія цього Порядку не поширюється на інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі, в яких обробляється службова інформація та/або інформація, що становить державну таємницю, розвідувальну таємницю, банківську таємницю [14].

Надано визначення таким поняттям: власник системи, вразливість системи, декомпіляція, дизасемблювання, дослідник потенційної вразливості, звіт про

вразливість системи за результатами пошуку її потенційної вразливості, зворотний інжиніринг, зміни до системи, координатор пошуку потенційної вразливості системи, період нерозголошення інформації про вразливість системи.

Основною метою постанови є встановлення структурованого підходу до аналізу та усунення вразливостей, якими можуть скористатися зловмисники для проведення кібератак. Пошук вразливостей має проводитися регулярно та відповідно до встановлених процедур, щоб забезпечити своєчасне виявлення та реагування на кіберінциденти.

2.8 Наказ Міністерства енергетики України «Про Вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури»

Ці Вимоги визначають заходи кіберзахисту об’єктів критичної інформаційної інфраструктури, що експлуатуються на об’єктах критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури для досягнення конкретного цільового стану кібербезпеки [15].

Надано визначення таким поняттям: активи, віртуальна приватна мережа, екосистема, профіль кіберзахисту, система (таксономія) заходів кіберзахисту.

Основною метою наказу є встановлення обов'язкових вимог до організацій, які здійснюють діяльність у паливно-енергетичному секторі, щодо забезпечення належного рівня кібербезпеки. Вимоги включають проведення заходів з попередження, виявлення, реагування на кіберінциденти, а також відновлення роботи систем після можливих атак. Документ вимагає впровадження політик та процедур, які регулюють доступ до інформаційних ресурсів, управління ризиками та реагування на інциденти.

2.9 Постанова Кабінету Міністрів України від 23 серпня 2016 р. № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави»

Цей Порядок визначає механізм формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави [17].

Надано визначення таким поняттям: заінтересовані органи, кібератака, контрольована зона, критична інфраструктура, об’єкти критичної інфраструктури.

Основною метою постанови є забезпечення захисту інформаційних ресурсів критичної інфраструктури, від різних загроз, включаючи кібератаки, техногенні аварії та інші небезпеки. У документі сформовано перелік негативних наслідків до яких може призвести кібератака.

2.10 Постанова Кабінету Міністрів України від 9 жовтня 2020 р. N 1109 «Деякі питання об'єктів критичної інфраструктури»

Цей Порядок визначає механізм віднесення об'єктів до об'єктів критичної інфраструктури та їх категоризації.

Надано визначення таким поняттям: безпека об'єкта критичної інфраструктури, власник та/або керівник об'єкта критичної інфраструктури, життєво важливі послуги та функції, захист об'єктів критичної інфраструктури, ідентифікація об'єкта критичної інфраструктури, категоризація об'єктів критичної інфраструктури, категорія критичності об'єкта критичної інфраструктури, кризова ситуація, критична інфраструктура, сектор (підсектор) критичної інфраструктури, уповноважений орган державної влади, відповідальний за сектор (підсектор) критичної інфраструктури (далі - уповноважений орган), час відновлення.

Документ надає:

- перелік віднесення об'єктів до об'єктів критичної інфраструктури;
- перелік секторів (підсекторів), основних послуг критичної інфраструктури держави;
- методику категоризації об'єктів критичної інфраструктури;
- додаток 1 до методики: визначення рівня негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури (секторальні критерії);
- додаток 2 до методики: визначення рівня негативного впливу у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури (міжсекторальні критерії).

3 РОЗРОБКА РЕКОМЕНДАЦІЙ СТОСОВНО ПІДТРИМКИ АКТУАЛЬНОСТІ АПАРАТНОГО ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Сервери, мережеве обладнання, спеціалізовані програмні платформи і служби є складовими ІТ структури і потребують проведення регулярної модернізації ІТ сервісів до мінливих в сучасних динамічних ринкових умовах потребам бізнес-діяльності підприємства.

Впровадження уніфікованих рішень для забезпечення безпеки і гнучкого контролю всіх робочих станцій, пристроїв і додатків, інтегровані програмні рішення для захисту важливої корпоративної інформації та управління критичними ризиками на єдиній платформі являють собою єдину інноваційну платформу для забезпечення безпеки кінцевих точок – від антивірусу, контролю додатків і знімних носіїв до інтелектуального менеджменту, управління ІТ-ризиками та перевірки на відповідність політикам і стандартам безпеки.

Однією з ключових тенденцій в розвитку ІТ інфраструктури можна вважати зростання вимог до надійності і продуктивності обчислювальної інфраструктури з регулярним збільшенням пропускної спроможності каналів передачі даних і обсягу оброблюваних корпоративних даних.

Цільове призначення корпоративної інформаційної системи полягає в інформаційному супроводі діяльності підприємства. Базисом системи є загальносистемне програмне забезпечення, яке включає операційну систему і програмні оболонки, програми загального і прикладного призначення: автоматизовані робочі місця і веб-сервіси загального та спеціального призначення, СУБД і управління інтегрованими обчислювальними і мультимедійними додатками, а також доступом в локальні і зовнішні мережі.

Нижній рівень корпоративної інформаційної системи базується на серверах, робочих станціях, персональних комп'ютерах різного призначення і комунікаційних пристроях, а також на програмному забезпеченні, що підтримує роботу перерахованих пристроїв.

3.1 Оновлення комп’ютерної техніки та програмного забезпечення

Системний блок є основним компонентом комп'ютера, який містить усі необхідні для його роботи деталі. Через 5 років експлуатації комп’ютер, якщо ще є працездатним, то в зв’язку з впровадженням нових сучасних програм, які потребують набагато більше технічних ресурсів, вже вважається застарілим обладнанням і потребує заміни.

Згідно з Постановою Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури», у складі об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинно використовуватися програмне та апаратне забезпечення, для якого не припинено підтримку виробника [5].

Відповідно до затвердженого документу на одному з критичних підприємств планується заміна комп’ютерної техніки [6].

Таблиця 3.1 – Мінімальні вимоги до компонентів комп’ютера згідно з документацією підприємства

Компонент	**Мінімально необхідні характеристики**
Оперативна пам'ять (ОЗП)	– Ємність: 8 GB – Тип: DDR4 – Частота 2400 МГц

Продовження таблиці 3.1

1	2
Процесор (ЦПУ)	– Кількість ядер: 4 – Частота: 3200 МГц
Пристрій збереження даних	– Тип: SSD – Об’єм: 256 ГБ
Мережева карта	– Швидкість: Gigabit Ethernet (1 Gbps) – Кількість портів: 1 RJ-45
Відеокарта	– Об'єм: 6 GB – Тип: GDDR5
Дисплей	– Діагональ: 15,6"

Базуючись на даних з таблиці 3.1 визначено підходящі моделі компонентів комп’ютерів.

Таблиця 3.2 – Рекомендовані моделі компонентів настільного комп’ютера.

Компонент	Модель
Оперативна пам'ять (ОЗП)	GOODRAM (GR2400D464L17S/8G)
Процесор (ЦПУ)	AMD Ryzen 3 4300GE (3.5GHz 4MB 35W AM4) (100-100000151MPK)

Продовження таблиці 3.2

1	2
Пристрій збереження даних	SSD Kingston KC600 256GB 2.5" SATAIII 3D NAND TLC (SKC600/256G)
Мережева карта	Edimax EN-9235TX-32 V2
Відеокарта	Zotac GTX 1060 6Gb AMP Edition! (ZT-P10600B-10M) "Seller Refurbished"
Дисплей	15.6" ASUS VT168HR (90LM02G1-B04170)

Окрім апаратної складової, необхідно також перевірити актуальність встановлених операційних систем та у разі необхідності оновити і їх. Політики життєвого циклу системного ПЗ компанії Microsoft встановлюють чіткі та і правила щодо термінів підтримки продуктів та обслуговування [7].

Таблиця 3.3 – Життєвий цикл операційних систем Microsoft для ПК

Операційна система	Дата завершення підтримки
Windows XP	8 квіт. 2014 р.
Windows 7	14 січ. 2020 р.
Windows 8	12 січ. 2016 р.
Windows 10	14 жовт. 2025 р.
Windows 11	2031 р.

На даний момент немає офіційної інформації щодо завершення терміну підтримки Windows 11, оскільки Microsoft ще не вирішила щодо цього. Однак, зазвичай, ОС Windows підтримується приблизно 10 років після запуску. Оскільки Windows 11 було запущено в 2021 році, то завершення терміну служби очікується в 2031 році.

Після припинення активного розвитку операційної системи розробники продовжують підтримувати його в актуальному стані шляхом випуску важливих оновлень, включаючи так звані оновлення безпеки. Наприкінці життєвого циклу програмного забезпечення розробники продовжують випускати лише критично важливі оновлення безпеки, які усувають відомі вразливості. Пристрої, операційні системи яких не отримують оновлень, є вразливішими до атак зловмисників.

Також, компанія Microsoft випускає щомісячні оновлення системи безпеки у другий вівторок кожного місяця. Щомісячні оновлення є накопичувальними та містять усі раніше випущені виправлення для захисту від фрагментації операційної системи (ОС). Це сприяє надійності та якості платформи Windows. Щомісячні оновлення системи безпеки є обов'язковими та доступні через такі канали: Windows Update, Microsoft Intune, Windows Server Update Services (WSUS), Microsoft Configuration Manager, Windows Update for Business, і Microsoft Update Catalog.

Коли виявлено вразливість безпеки або проблему з якістю, і з'являється потреба у негайному виправленні, то Microsoft може надати реліз раніше дати запланованого щомісячного оновлення.

Windows 11 має щорічну періодичність оновлення функцій. Оновлення функцій виходять у другій половині календарного року та забезпечують 24-

місячну підтримку версій Home, Pro, Pro for Workstations і Pro Education; 36 місяців підтримки версій Enterprise і Education.

Так само щорічно оновлення функцій випускаються і для випуску Windows 10, у другій половині календарного року. Однак вони обслуговуватимуться щомісячними оновленнями якості протягом 18 або 30 місяців із дати випуску, залежно від політики життєвого циклу.

Виходячи з даних Таблиці 3.3, актуальними на даний час є операційні системи Windows 10 та Windows 11. Так як термін підтримки Windows 11 є більшим, то доцільніше встановлювати саме цю ОС версії Pro.

Спираючись на інформацію з офіційної сторінки Microsoft, порівняємо мінімальні вимоги до системи, які необхідні для правильного функціонування Windows 11 Pro з мінімально необхідними вимогами підприємства.

Таблиця 3.4 – Порівняння вимог

Компонент	**Мінімально необхідні характеристики**	**Вимоги Microsoft**
Оперативна пам'ять (ОЗП)	– Ємність: 8 GB – Тип: DDR4 – Частота 2400 МГц	– Ємність: 4 GB
Процесор (ЦПУ)	– Кількість ядер: 4 – Частота: 3200 МГц	– Кількість ядер: 2 – Частота: 1100 МГц
Пристрій збереження даних	– Тип: SSD – Об’єм: 256 ГБ	– Об’єм: 64 Гб
Дисплей	– Діагональ: 15,6"	– Діагональ: 9"

Проаналізувавши Таблицю 3.4, бачимо, що Windows 11 підходить для встановлення на оновленому обладнанні.

На обраному критичному підприємстві користувачі ПК працюють з пакетом Microsoft Office. Оновлення програмного забезпечення важливі для Microsoft Office так само, як і для інших програм та ОС.

Важливі виправлення зазвичай входять до оновлення ПЗ, що забезпечує безпеку даних користувачів. Якщо регулярно встановлювати оновлення – отримуємо оновлення для системи безпеки і захист від атаки. Також якщо використовується застаріла версію програми, яка не підтримує останні оновлення, це теж може стати проблемою – необхідно перейти на сучасну версію програми, яка підтримує всі оновлення.

Застарілі версії Microsoft Office можуть мати неточності в безпеці. Наприклад, застаріла версія Microsoft Outlook вразлива до шкідливих електронних листів, а застаріла версія Microsoft Word вразлива до шкідливих документів DOC і DOCX, які можливо завантажити та відкрити. Навіть шкідливе зображення, яке копіюється та вставляєте в документ Office, може потенційно зашкодити операційній системі, якщо відсутні останні оновлення. Застаріла копія Word 2000 може як і раніше відповідати всім потребам, але у неї є недоліки безпеки, які можна використовувати. Якщо завантажити і відкрити шкідливий файл, він може встановити шкідливе ПЗ на комп’ютер. Виправлення безпеки в більш нових версіях файлів усунули цю проблему. Тому на нові ПК з новою ліцензійною операційною системою потрібен новий пакет ПЗ Microsoft Office.

Таблиця 3.5 – Життєвий цикл пакету ПЗ Microsoft Office

Пакет ПЗ Microsoft Office	**Дата завершення підтримки**
Microsoft Office 2003	08 квіт. 2014 р.
Microsoft Office 2007	10 жовт. 2017 р.
Microsoft Office 2010	13 жовт. 2020 р.
Microsoft Office 2013	11 квіт. 2023 р.
Microsoft Office 2016	14 жовт. 2025 р.
Microsoft Office 2019	14 жовт. 2025

Відповідно до Таблиці 3.5 актуальними на даний час є пакети Microsoft Office 2016 та Microsoft Office 2019, тому рекомендовано встановлювати саме їх.

3.2 Оновлення серверного та мережевого обладнання

Центри обробки даних займають центральне місце в IT-інфраструктурі. Правильне планування та проектування є критично важливим завданням, так як і продуктивність, відмовостійкість, масштабованість повинні бути ретельно продумані.

Основним завданням ЦОД є:

- забезпечення відмовостійкості з’єднань з серверами і системами зберігання даних (СЗД), що дозволяє підняти ефективність, надійність і забезпечити безперервність ведення критичних бізнес-процесів;
- забезпечення масштабованості і гнучкості нарощування обчислювальних потужностей, які ідеально відповідають зростаючим бізнес-потребам замовника;

– спрощення інтеграції з іншими модулями мережевої інфраструктури, що зменшує витрати на впровадження і подальше обслуговування.

Згідно з Постановою Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури», для захисту об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні використовуватися програмно-апаратні засоби, потужність яких визначається виходячи із потужності трафіку, який передбачається в мережі, з урахуванням його потенційного збільшення [5].

Сучасне серверне обладнання критичного об’єкта повинно забезпечити роботу програмних комплексів, сервісів та інформаційних ресурсів, таких, як: АСКУЕ споживачів електроенергії, послуги приєднання, колцентр, управління виробництвом, АСУТП, система електронного документообігу та інші. Так як навантаження на сервери постійно збільшується, необхідно проводити переоснащення серверних платформ.

Таблиця 3.6 – Мінімальні вимоги до сервера згідно з документацією підприємства

Компонент	**Мінімально необхідні характеристики**
Процесор	– Частота: 2,6 ГГц – Кількість ядер: 26 – Модель: Intel® Xeon

Продовження таблиці 3.6

1	2
Оперативна пам’ять	– Обсяг: 256 ГБ – Тип: DDR4
Інші вимоги: – швидко розгортати середовища віртуалізації за рахунок підтримки вбудованих гіпервізора провідних розробників, що запускаються з карти пам'яті SD або внутрішнього устрою USB. – підтримувати технологію Intel® VT FlexMigration, яка дозволяє інтегрувати сервери різних поколінь з процесорами Intel® Xeon®, сприяючи підвищенню гнучкості і додаткового захисту інвестицій. – підтримувати технологію Energy Smart™, орієнтовану на скорочення енергоспоживання одночасно з підвищенням продуктивності. – мати вбудовані системи керування Dell EMC, що забезпечують інтелектуальне, автоматизоване управління серверами, системами зберігання даних, мережевими модулями і середовищами модульних інфраструктур. – підтримувати гарячу заміну HDD (Hot Plug); – підтримувати гарячу заміну БЖ (Hot Plug).	

Базуючись на даних з таблиці 3.6 визначено підходящу модель серверів, а саме Dell EMC PowerEdge R740xd. Це високопродуктивний сервер 14-го покоління, який був випущений у 2019 році. Компанія Dell поки що не надала задокументованої інформації про кінець терміну підтримки рекомендованої моделі. Зазвичай, термін служби сервера Dell становить близько 5-7 років з дати

покупки, це також залежить від наявності запчастин і обслуговування в регіонах. Щойно закінчиться гарантія на продукт, компанія направляє електронний лист або дзвінок для поновлення. Може бути пріоритетна підтримка та обмежені періоди підтримки [21].

Нові сервери з поліпшеними можливостями обробки даних, вдосконаленим сховищем, більш швидкими можливостями введення/виведення і підвищеним обсягом пам'яті дозволяють швидше і ефективніше запускати клієнтські програми і процеси, а також усувати проблеми, пов'язані з робочими навантаженнями.

Оновлені сервери мають бути оснащенні актуальними ОС.

Таблиця 3.7 – Життєвий цикл операційних систем Microsoft для серверного обладнання

Операційна система	**Дата завершення підтримки**
Windows Server 2003	14 лип. 2015 р.
Windows Server 2008	14 січ. 2020 р.
Windows Server 2012	10 жовт. 2023 р.
Windows Server 2016	12 січ. 2027 р.
Windows Server 2019	09 січ. 2029 р.
Windows Server 2022	14 жовт. 2031

Відповідно до Таблиці 3.7 актуальними на даний час є Windows Server 2016, Windows Server 2019, Windows Server 2022. Остання є найновішою версією

і пропонує найсучасніші функції та можливості, тому рекомендовано придбати ліцензії саме на ОС Windows Server 2022.

Починаючи з вересня 2023 р. у Windows Server є два основних канали випуску: канал обслуговування довгостроковий (Long-Term) і річний канал (Annual Channel). Канал обслуговування Long-Term надає більш довгостроковий варіант, орієнтований на стабільність, тоді як щорічний канал надає більш часті випуски [20].

У каналі обслуговування Long-Term нова основна версія Windows Server зазвичай випускається кожні 2-3 роки. Користувачі мають 5 років основної підтримки та 5 років розширеної підтримки. Цей канал надає системи з тривалим варіантом обслуговування та узгодженості та може бути встановлений із серверним ядром або сервером із параметрами встановлення робочого столу.

Annual Channel надає право клієнтам перейти до нових можливостей операційної системи у швидшому темпі. Кожне оновлення підтримується протягом 24 місяців із початкового випуску. Щорічний канал можна встановити лише за допомогою установки основних серверних компонентів. Це не є оновленням, а є наступним випуском Windows Server.

Таблиця 3.8 - Основні відмінності каналів обслуговування Long-Term та Annual Channel.

Критерій	**Long-Term**	**Annual Channel**
Нові випуски	2-3 роки	12 місяців
Підтримка	5 років основної підтримки, та 5 років розширеної підтримки	18 місяців основної підтримки, та 6 місяців розширеної підтримки

Продовження таблиці 3.8

1	2	3
Рекомендовані сценарії	Файлові сервери загального призначення, інфраструктурні ролі, програмно-визначені центри обробки даних та гіперконвергентна інфраструктура.	Контейнерні програми, що працюють на вузлах контейнерів, отримують переваги від більш швидких інновацій

Для впровадження мережевої безпеки необхідно також оновити застаріле мережеве обладнання, а саме комутатори та маршрутизатори.

Мінімальні вимоги до комутатора згідно з документацією підприємства:

- Оперативна пам’ять: 8 ГБ;
- Пам’ять FLASH: 16 ГБ;
- Процесор Intel x86;
- Кількість портів: 24 порти RJ-45;
- Підтримка VLAN.

Рекомендованою моделлю комутатора є Cisco C9300L-24T-4X-A. На даний момент немає інформації щодо кінцевої дати його підтримки. Відповідно до специфікації комутаторів Cisco, гарантійна підтримка обмежується 5 роками з моменту оголошення припинення виробництва продукту [9]. Рекомендована модель на даний момент виробляється, тому є актуальною.

Комутатор Cisco C9300L-24T-4X-A підтримує операційну систему Cisco IOS XE. У квітні 2024 року вийшло оновлення даної ОС до версії Cisco IOS-XE 17.14.1. Станом на зараз це найновіша версія. Випуски програмного забезпечення Cisco IOS XE 17.xx відбуваються кожні 4 місяця.

Кожна версія програмного забезпечення Cisco IOS XE класифікується як версія стандартної підтримки або версія розширеної підтримки [22].

- Стандартна: тривалість підтримки протягом 12 місяців із моменту першої поставки замовником (FCS) із запланованими перебудовами.
- Розширена: тривалість підтримки протягом 48 місяців із моменту першої поставки замовником (FCS) із запланованими перебудовами [22].

Версія Cisco IOS-XE 17.14.1 відноситься до версії розширеної підтримки. Інструкції щодо завершення продажу і завершення терміну служби програмного забезпечення Cisco IOS XE містять попередньо встановлені часові інтервали для кожного етапу терміну служби. [22]

Таблиця 3.9 – Етапи завершення продажу та завершення життєвого циклу програмного забезпечення Cisco IOS XE за випусками.

Етап	**Визначення**	**Час**
Перша відправка клієнту	Дата, коли випуск програмного забезпечення Cisco IOS XE стане доступним для клієнтів Cisco.	Початок терміну дії випуску програмного забезпечення Cisco IOS XE

Продовження таблиці 3.9

1	2	3
Дата оголошення про закінчення терміну експлуатації	Дата, коли документ, який сповіщає про припинення продажу та закінчення терміну служби продукту, розповсюджується серед широкої громадськості.	12 місяців після релізу
Дата закінчення продажу	Останній термін замовлення продукту. Після цієї дати продукт більше не продається.	6 місяців із дати оголошення про завершення терміну служби
Дата випуску завершення обслуговування програмного забезпечення	Остання дата, коли розробники Cisco можуть випустити випуск програмного забезпечення для обслуговування або запланований засіб для виправлення критичних помилок у випуску програмного забезпечення Cisco IOS XE.	12 місяців після дати завершення продажу

Продовження таблиці 3.9

1	2	3
Дата закінчення підтримки безпеки	Остання дата, коли розробники Cisco можуть випустити оновлення для обслуговування або усунення вразливості системи безпеки.	30 місяців після дати завершення продажу
Остання дата підтримки	Остання дата отримання обслуговування та підтримки продукту. Після цієї дати всі служби підтримки для продукту будуть недоступні, і продукт застаріє.	3 роки після дати завершення продажу

Наступним кроком є оновлення маршрутизаторів.

Таблиця 3.10 – Мінімальні вимоги до маршрутизатора згідно з документацією підприємства:

Компонент	Мінімально необхідні характеристики
Процесор	– Частота: 1700 МГц – Кількість ядер: 4

Продовження таблиці 3.10

1	2
Оперативна пам’ять	– Об’єм: 4 ГБ – Тип: DDR4
Інші вимоги: Мати вбудований міжмережевий екран (фаєрвол)	

Спираючись на дані, наведені в таблиці 3.10, визначено, що підходящою моделлю маршрутизатора є MikroTik Cloud Core Router CCR2004-16G-2S+. Маршрутизатори фірми Mikrotik містять безкоштовні оновлення програмного забезпечення протягом усього терміну служби продукту або щонайменше 5 років з дати покупки [10].

На пристроях Mikrotik попередньо встановлена та ліцензована операційна система. Не потрібно купувати окремо, продукт готовий до використання. Рекомендована модель підтримує операційну систему RouterOS v7. Станом на зараз найновішою версією є RouterOS v7.15, яка вийшла у травні 2024 року. Компанія Mikrotik не надає офіційної інформації стосовно термінів підтримки ОС. Важливо регулярно перевіряти доступні оновлення та вчасно встановлювати їх для забезпечення безпеки та стабільності мережі.

ВИСНОВКИ

У кваліфікаційній роботі було проаналізовано визначення такого поняття як критична інфраструктура, виконано огляд чинних в Україні нормативно-правових актів у сфері кіберзахисту об’єктів критичної інфраструктури. Також, було проведено ознайомлення з внутрішньою документацією об’єкта критичної інфраструктури енергетично-паливного сектору. Надано рекомендації стосовно підтримки актуальності апаратного та програмного забезпечення відповідно до вимоги чинного законодавства і таким чином розширено документ щодо планових заходів кіберзахисту.

Результатом роботи є таблиця, яка містить необхідні дані для оновлення апаратного і програмного забезпечення інформаційно-комунікаційної системи на об’єкті. Вона наведена у Додатку А.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про критичну інфраструктуру [Електронний ресурс] : Закон України від 16.11.2021 р. № 1882-IX : станом на 1 січ. 2024 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 30.05.2024). – Назва з екрана.
2. Про електроенергетику [Електронний ресурс] : Закон України від 16.10.1997 р. № 575/97-ВР : станом на 1 лип. 2019 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/575/97-вр#Text (дата звернення: 30.05.2024). – Назва з екрана.
3. Регіональна економіка : підручник / Гавкалова Н. Л., Гіковата Н. К., Петряєв О. О. та ін. ; за заг. ред. д.е.н. Н. Л. Гавкалової. – Х. : ВД "ІНЖЕК", 2011. – 464 с
4. Про нафту і газ [Електронний ресурс] : Закон України від 12.07.2001 р. № 2665-III : станом на 1 січ. 2024 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2665-14#Text (дата звернення: 30.05.2024). – Назва з екрана.
5. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури [Електронний ресурс] : Постанова Каб. Міністрів України від 19.06.2019 р. № 518 : станом на 7 верес. 2022 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text (дата звернення: 30.05.2024). – Назва з екрана.
6. Об'єктивні планові заходи кіберзахисту. – [Б. м. : б. в.]. – 41 с.
7. Microsoft Lifecycle [Електронний ресурс] // Microsoft Learn: Build skills that open doors in your career. – Режим доступу: https://learn.microsoft.com/uk-ua/lifecycle/products/export/ (дата звернення: 30.05.2024). – Назва з екрана.
8. Про затвердження Положення про організаційно-технічну модель кіберзахисту [Електронний ресурс] : Постанова Каб. Міністрів України від

29.12.2021 р. № 1426. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1426-2021-п#Text (дата звернення: 30.05.2024). – Назва з екрана.

9. Cisco Catalyst 9300 Series Switches Data Sheet [Електронний ресурс] // Cisco. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html#Warranty (дата звернення: 30.05.2024). – Назва з екрана.
10. CCR2216-1G-12XS-2XQ | MikroTik [Електронний ресурс] // MikroTik Routers and Wireless. – Режим доступу: https://mikrotik.com/product/ccr2216_1g_12xs_2xq#fndtn-specifications (дата звернення: 30.05.2024). – Назва з екрана.
11. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом [Електронний ресурс] : Постанова Каб. Міністрів України від 11.11.2020 р. № 1176. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1176-2020-п#Text (дата звернення: 30.05.2024). – Назва з екрана.
12. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки [Електронний ресурс] : Постанова Каб. Міністрів України від 23.12.2020 р. № 1295 : станом на 7 верес. 2022 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1295-2020-п#Text (дата звернення: 30.05.2024). – Назва з екрана.
13. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі [Електронний ресурс] : Постанова Каб. Міністрів України від 04.04.2023 р. № 299. – Режим доступу:

https://zakon.rada.gov.ua/laws/show/299-2023-п#Text (дата звернення: 30.05.2024). – Назва з екрана.

14. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж [Електронний ресурс] : Постанова Каб. Міністрів України від 16.05.2023 р. № 497. – Режим доступу: https://zakon.rada.gov.ua/laws/show/497-2023-п#Text (дата звернення: 30.05.2024). – Назва з екрана.
15. Про Вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури [Електронний ресурс] : Наказ М-ва енергетики України від 15.12.2022 р. № 417. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0249-23#Text (дата звернення: 30.05.2024). – Назва з екрана.
16. Про затвердження Кодексу системи передачі [Електронний ресурс] : Постанова Нац. коміс., що здійснює держ. регулювання у сферах енергетики та комун. послуг від 14.03.2018 р. № 309 : станом на 16 лют. 2024 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v0309874-18#Text (дата звернення: 30.05.2024). – Назва з екрана.
17. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави [Електронний ресурс] : Постанова Каб. Міністрів України від 23.08.2016 р. № 563 : станом на 22 жовт. 2020 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/563-2016-п#Text (дата звернення: 30.05.2024). – Назва з екрана.
18. Деякі питання об'єктів критичної інфраструктури [Електронний ресурс] : Постанова Каб. Міністрів України від 09.10.2020 р. № 1109 : станом на 20

січ. 2024 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text (дата звернення: 30.05.2024). – Назва з екрана.

19. Windows 11 - release information [Електронний ресурс] // Microsoft Learn: Build skills that open doors in your career. – Режим доступу: https://learn.microsoft.com/en-us/windows/release-health/windows11-release-information (дата звернення: 30.05.2024). – Назва з екрана.
20. Windows Server release information [Електронний ресурс] // Microsoft Learn: Build skills that open doors in your career. – Режим доступу: https://learn.microsoft.com/en-us/windows/release-health/windows-server-release-info (дата звернення: 30.05.2024). – Назва з екрана.
21. Dell PowerEdge End OF Life and End of Support Server List [Електронний ресурс] // DellTechnologies. – Режим доступу: https://www.dell.com/community/en/conversations/rack-servers/dell-poweredge-end-of-life-and-end-of-support-server-list/647f94b2f4ccf8a8de70e717 (дата звернення: 30.05.2024). – Назва з екрана.
22. Software Lifecycle Support Statement - IOS XE [Електронний ресурс] // cisco. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-xe-16/bulletin-c25-2378701.html (дата звернення: 30.05.2024). – Назва з екрана.

Додаток А

Таблиця А.1 – Рекомендаційні оновлення апаратного та програмного забезпечення на об’єкті критичної інфраструктури відповідно до чинного законодавства України

Апаратна складова		**Програмна складова**	
Пристрій	**Модель**	**Операційна система**	**ПЗ**
Настільний персональний комп’ютер	Оперативна пам'ять GOODRAM (GR2400D464L17S/8G)	Windows 11 Pro	Microsoft Office 2019
	Процесор AMD Ryzen 3 4300GE (3.5GHz 4MB 35W AM4) (100-100000151MPK)		
	Пристрій збереження даних SSD Kingston KC600 256GB 2.5" SATAIII 3D NAND TLC (SKC600/256G)		
	Мережева карта: Edimax EN-9235TX-32 V2		

	Відеокарта Zotac GTX 1060 6Gb AMP Edition! (ZT-P10600B-10M) "Seller Refurbished"		
	Дисплей: 15.6" ASUS VT168HR (90LM02G1-B04170)		
Пристрій	**Модель**	**Операційна система**	
Сервер	Dell EMC PowerEdge R740xd	Windows Server 2022	
Комутатор	Cisco C9300L-24T-4X-A	Cisco IOS-XE 17.14.1	
Маршрутизатор	MikroTik Cloud Core Router CCR2004-16G-2S+.	RouterOS v7.15	