DOI https://doi.org/10.36059/978-966-397-413-2-9

РОЗДІЛ 9
ІНТЕГРАЦІЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У СИСТЕМУ БЕЗПЕКИ: АДАПТАЦІЯ ДО НОВИХ ВИКЛИКІВ І МОЖЛИВОСТЕЙ

(д.ф.н., проф. Воронкова В. Г., д.е.н.,проф. Метеленко Н. Г., д.н.держ. управ., проф. Ажажа М. А., д.п.н., проф. Арабаджиєв Д.Ю, д.ф.н., проф. Нікітенко В. О., здобувач PhD Дашков А. О., к.п.н., доц. Венгер О. М., к.н.держ.управ., доц. Фурсін О. О., к. фарм.н., доц. Шарапова Т. А., здобувач PhD Цикін Д. С.)

Види безпеки можна класифікувати за різними критеріями. Виділимо основні види безпеки: 1) Національна безпека: політична безпека; військова безпека; економічна безпека; енергетична безпека; інформаційна безпека; екологічна безпека; соціальна безпека. 2) Економічна безпека: фінансова безпека; технологічна безпека; продовольча безпека; ресурсна безпека. 3) Особиста безпека: фізична безпека; психологічна безпека; соціальна безпека. 4) Інформаційна безпека: захист інформаційних систем; кібербезпека; конфіденційність даних. 5) Екологічна безпека: безпека навколишнього середовища; радіаційна безпека; хімічна безпека. 6) Технологічна безпека: інженерна безпека; промислова безпека; техногенна безпека. 7) Глобальна безпека: міжнародна безпека; колективна безпека; глобальні загрози (тероризм, кліматичні зміни). Кожен з цих видів безпеки має свої специфічні аспекти та підходи до забезпечення. Мета дослідження – систематизувати підходи теоретичного узагальнення наукових поглядів забезпечення безпеки в умовах викликів, можливостей та змін.

9.1 СОЦІАЛЬНО-ЕКОНОМІЧНА БЕЗПЕКА

Актуальність дослідження соціально-економічної безпеки з врахуванням європейських практик в умовах викликів, можливостей та змін забезпечує стабільність та розвиток суспільства через ефективне

управління економічними і соціальними процесами та досягнення національної безпеки. Соціально-економічна безпека охоплює широкий спектр питань, включаючи економічну стабільність, соціальний захист, зайнятість, охорону здоров'я, освіту, захист прав та свобод громадян, а також забезпечення рівного доступу до ресурсів і можливостей. Соціально-економічна безпека базується на комплексному підході та співпраці між державою, бізнесом, громадянським суспільством та міжнародними організаціями. Важливим є розробка та впровадження соціально-економіення ефективних політик, що сприятимуть збалансованому розвитку суспільства та економіки, а також забезпечать захист та добробут громадян.

Соціально-економічна безпека є передумовою розвитку, який є гарантією національної безпеки, а координація розвитку та безпеки, а також сприяння високоякісному розвитку невіддільні від сталого та стабільного середовища безпеки. Соціально-економічна безпека є важливим проявом модернізації систем та можливостей національної безпеки. Уряди повинні рішуче захищати інтереси розвитку своїх країн, активно захищатись від різних ризиків та забезпечувати є підтримка економічної безпеки, особливо продовольчої безпеки, енергетичної безпеки, безпеки постачання промислового ланцюжка, що відображають глибоке розуміння основних законів національної безпеки і дають фундаментальні орієнтири для забезпечення економічної безпеки в нову епоху і на новому шляху.

Таблиця 9.1 – Основні аспекти соціально-економічної безпеки

Основні аспекти	**Зміст основних аспектів соціально-економічної безпеки**
Економічна стабільність	Забезпечення стійкого економічного зростання. Контроль інфляції та підтримка стабільності національної валюти. Зменшення залежності від зовнішніх економічних чинників.
Зайнятість і ринок праці	Підтримка високого рівня зайнятості. Розвиток системи перекваліфікації та навчання робочої сили. Захист прав працівників.
Соціальний захист	Розвиток системи соціального страхування. Підтримка вразливих верств населення. Забезпечення доступу до якісної охорони здоров'я та освіти.
Інституційна безпека	Зміцнення державних інститутів. Протидія корупції та тіньовій економіці. Підтримка правової держави та верховенства права.
Екологічна безпека	Захист навколишнього середовища. Підтримка стійкого розвитку. Протидія кліматичним змінам.

Як свідчить системний аналіз зарубіжних і вітчизняних джерел, під соціально-економічною безпекою розуміється здатність національної економіки протистояти різним внутрішнім та зовнішньоекономічним ризикам та підтримувати стабільну та впорядковану діяльність. Це є важливою частиною системи національної безпеки, яка є найважливішим завданням захисту національних економічних інтересів та довгострокових інтересів народу, необхідною гарантією якісного розвитку та побудови сучасної економічної системи. Тільки зміцнюючи національну економічну безпеку та сприяючи стійкому та здоровому економічному розвитку, уряди зможуть створити міцну матеріальну основу для національного процвітання, благополуччя людей, соціальної гармонії та стабільності.

Соціально-економічна безпека є комплексним і багатогранним поняття та концепцією, що вимагає стратегічного підходу та співпраці різних секторів суспільства. Її забезпечення є ключовим фактором стабільного та стійкого розвитку держави, що сприяє підвищенню якості життя населення та забезпеченню майбутніх поколінь. Європейські практики діджиталізації як інструмент забезпечення соціально-економічної безпеки включають: 1) Багато країн в Європі активно впроваджують електронні системи урядування, що спрощує надання громадянських послуг, зменшує бюрократію та покращує взаємодію між урядом і громадянами. 2) Європейські країни інвестують у цифрову освіту, щоб готувати молодь до цифрової економіки та забезпечувати їхню конкурентоспроможність на ринку праці. 3) Розвиток швидкого та надійного Інтернету, а також інших цифрових технологій, є важливим аспектом забезпечення соціально-економічної безпеки. 4) Європейські країни впроваджують технології у сфері охорони здоров'я, такі як електронні медичні картки, телемедицину та інші цифрові інструменти для покращення якості та доступності медичних послуг. 5) Забезпечення безпеки цифрових систем та захист особистих даних громадян є ключовим аспектом соціальноекономічної безпеки. 6) Розвиток цифрових технологій, інновацій та 397 підтримка стартапів сприяють росту економіки та створенню нових робочих місць. 7) Використання інтернету речей (IoT) та інших цифрових рішень для покращення ефективності міського управління в смарт-сіті сприяє зменшенню екологічного впливу та підвищенню якості життя громадян.

Європейські практики діджиталізації як інструмент забезпечення соціально-економічної безпеки спрямовані на створення більш стабільного, конкурентоспроможного та безпечного суспільства в умовах цифрової трансформації. Забезпечення соціально-економічної безпеки» включає комплекс заходів, спрямованих на досягнення стійкості та безпеки суспільства в економічній та соціальній сферах.

Таблиця 9.2 – Виклики соціально-економічній безпеці

Виклики	Зміст та характеристика
Глобалізація	Посилення конкуренції на світових ринках. Вплив транснаціональних корпорацій. Фінансові кризи та їхній вплив на національні економіки.
Технологічні зміни	Автоматизація та роботизація виробництва. Цифрова трансформація економіки та суспільства. Захист персональних даних та інформаційна безпека.
Соціальні нерівності	Розрив між багатими та бідними. Доступ до освіти, охорони здоров'я та інших соціальних послуг. Дискримінація та соціальна ізоляція.
Демографічні зміни	Старіння населення. Міграційні процеси. Зміна структури родин та домогосподарств.

Це включає в себе різноманітні політики, програми і дії, спрямовані на покращення економічної стабільності, забезпечення достатку населення, соціальної справедливості, охорони здоров'я, освіти, працевлаштування та інших аспектів життя суспільства. Європейські практики діджиталізації як інструмент забезпечення соціально-економічної безпеки включають різні стратегії, програми та ініціативи, спрямовані на використання цифрових технологій для поліпшення економічних та соціальних показників.

Таблиця 9.3 – Стратегії забезпечення соціально-економічної безпеки

Напрям стратегії	Зміст та характеристика
1	2
Економічна політика: фіскальна, монетарна, промислова	Підтримка макроекономічної стабільності через ефективне управління державними фінансами, зменшення дефіциту бюджету та державного боргу. Контроль інфляції та підтримка стабільності національної валюти через регулювання грошово-кредитної системи. Стимулювання розвитку ключових галузей економіки, інновацій та технологічного прогресу.
Соціальна політика: системиа соціального захисту, охорона здоров'я, освіта	Розвиток програм соціального страхування, допомоги малозабезпеченим, підтримка безробітних та пенсійне забезпечення. Забезпечення доступу до якісних медичних послуг, розвиток профілактичних програм та охорони здоров'я. Підвищення якості освіти, забезпечення доступу до неї, підтримка наукових досліджень та інновацій.

Закінчення таблиці 9.3

1	2
Ринок праці: зайнятість, перекваліфікація, захист працівників	Підтримка високого рівня зайнятості через стимулювання створення нових робочих місць, розвиток малого та середнього бізнесу. Програми навчання та перекваліфікації робочої сили відповідно до потреб ринку праці. Підтримка прав працівників, забезпечення гідних умов праці та заробітної плати.
Екологічна безпека: стійкий розвиток, енергоефективність, кліматична політика	Впровадження принципів стійкого розвитку, що включає раціональне використання природних ресурсів, зменшення викидів шкідливих речовин та збереження біорізноманіття. Підвищення енергоефективності, розвиток відновлюваних джерел енергії. Реалізація заходів щодо протидії зміні клімату, адаптація до кліматичних змін.
Інституційна реформа: прозорість і підзвітність, зміцнення правової системи, електронне урядування	Розвиток системи прозорого та підзвітного державного управління, впровадження антикорупційних заходів. Забезпечення верховенства права, вдосконалення судової системи, захист прав і свобод громадян. Впровадження цифрових технологій в державне управління для підвищення ефективності та прозорості процесів.

Інформаційна безпека як складова соціально-економічної безпеки – стосується заходів і стратегій, спрямованих на захист інформації від небажаних доступів, втрати, пошкодження або несанкціонованого використання. Інформаційна безпека є важливою для організацій, компаній та індивідів, оскільки інформація може бути цінним активом для сталого розвитку підприємств та організацій.

Ці елементи інформаційної безпеки допомагають забезпечити надійний захист інформації в різних сферах, включаючи бізнес, уряд та особисте використання. Інформаційна безпека (InfoSec) пов'язана із захистом усієї важливої інформації організації (цифрових файлів і даних, паперових документів, фізичних носіїв і навіть людського втручання) від несанкціонованого доступу, розкриття, використання або зміни. Безпека даних, захист цифрової інформації, є підмножиною інформаційної безпеки та зосереджена на більшості заходів InfoSec, пов'язаних з кібербезпекою. Інформаційна безпека (InfoSec) передбачає захист усієї важливої інформації організації = цифрових файлів і даних, паперових документів, фізичних носіїв і навіть людського голосу – від несанкціонованого доступу, розголошення, використання або фальсифікації. Безпека даних, тобто захист цифрової інформації, є підмножиною інформаційної безпеки та фокусом більшості заходів інформаційної безпеки, пов'язаних з кібербезпекою.

Таблиця 9.4 – Складові інформаційної безпеки та їх характеристика

Складова інформаційної безпеки	Зміст та характеристика
Конфіденційність	Це забезпечення того, щоб інформація була доступною лише тим особам або сутностям, які мають право на доступ до неї. Для забезпечення конфіденційності можуть використовуватися шифрування, контроль доступу і інші технічні та організаційні заходи.
Цілісність	Цілісність інформації означає, що вона залишається недоторканою і не піддається несанкціонованим змінам або пошкодженням. Виявлення будь-яких змін в інформації і її відновлення в початковий стан є важливими аспектами цілісності.
Доступність	Ця складова інформаційної безпеки забезпечує, що інформація завжди доступна тим, хто має на це право. Доступність включає в себе заходи для запобігання відмовам в обслуговуванні, природнім катастрофам і іншим факторам, які можуть обмежити доступність інформації.
Аутентифікація	Аутентифікація визначає, чи є особа чи сутність, яка намагається отримати доступ до інформації, дійсно тією, за кого себе видає. Це може бути досягнуто за допомогою паролів, біометричних методів і інших ідентифікаційних засобів.
Авторизація	Авторизація визначає, які дії або операції може виконувати особа або сутність після успішної аутентифікації. Вона визначає права доступу до інформації та можливість виконання різних дій.
Невідкладність	Цей аспект інформаційної безпеки стосується здатності реагувати на ідентифікацію та усунення загроз, порушень або вразливостей в найкоротший можливий строк
Недефектність	Забезпечення безпеки програмного забезпечення та апаратного забезпечення, що використовується для обробки інформації, є важливим аспектом інформаційної безпеки. Це включає в себе заходи для запобігання вразливостям і використанню багатьох різних видів захисту.
Захист від загроз	Інформаційна безпека повинна враховувати різні види загроз, такі як кібератаки, віруси, хакерські атаки, фішинг і інші. Захист від таких загроз включає в себе використання антивірусного програмного забезпечення, мережевих брандмауерів, систем виявлення і запобігання інцидентам і інші заходи.

Таблиця 9.5 – Порівняльний аналіз міжнародного досвіду забезпечення соціально-економічної безпеки: країни Європейського Союзу, США, Китай

Складова інформаційної безпеки	Зміст та характеристика
Країни Європейського Союзу	Соціальна держава: ЄС активно підтримує розвиток соціальної держави, що включає високу якість соціальних послуг, широкий спектр соціальних гарантій та активну політику зайнятості. Європейська стратегія зайнятості: Координація політики зайнятості між країнами-членами, розвиток єдиного ринку праці. Екологічна політика: Впровадження Зеленої угоди, спрямованої на перехід до кліматично нейтральної економіки до 2050 року.
США	Економічна політика: Акцент на стимулювання економічного зростання через інновації, розвиток технологій та підприємництва. Соціальні програми: Розвиток системи соціального страхування, програм охорони здоров'я, підтримки безробітних. Екологічна політика: Підтримка відновлюваних джерел енергії, програми зменшення викидів парникових газів.
Китай	Економічне зростання: Стратегія стимулювання високих темпів економічного зростання через індустріалізацію, урбанізацію, розвиток інновацій та технологій. Соціальні реформи: Підтримка соціальної стабільності через розвиток системи соціального забезпечення, освіти, охорони здоров'я. Екологічна політика: Впровадження програм зменшення забруднення, розвиток зеленої економіки. Сильна стратегія кібербезпеки захищає всі відповідні рівні або області IT-інфраструктури від кіберзагроз і кіберзлочинності.

Хоча Китай випустив деякі документи стратегічного планування з кібербезпеки, в яких наголошується на важливості підготовки спеціалістів, загалом все ще бракує загального планування та дизайну на найвищому рівні у галузі кібербезпеки. На противагу цьому, Сполучені Штати вже мають провідну стратегію та систему мережевих спеціалістів, а також випустили Національну стратегію мережевих талантів та освіти, яка спрямована на сприяння реформі уряду, підприємств, шкіл та інших організацій у галузі навчання та розвитку талантів для задоволення поточних та майбутніх потреб мережевих спеціалістів, що матиме далекосяжний вплив на міжнародну кібербезпеку. Європейські країни стикаються з більш жорсткою та складною конкурентною ситуацією у сферах міжнародних правил кіберпростору та індустрії інформаційних технологій, що принесло нові виклики участі та домінування Китаю у формулюванні правил кіберпростору.

Постійне просування нових технологічних додатків, таких як Інтернет речей, мобільний Інтернет, навігація та позиціонування, принесло нові проблеми безпеки в будівництво нових розумних міст, а Інтернет, Інтернет речей та великі дані ще більше посилили взаємозалежність безпеки між кіберпростором та фізичним простором. Міська мережа є сполучною ланкою між фізичним містом та цифровим містом-побратимом, яке є не лише ключовою наріжною базою та центром цифрового транспорту для розвитку розумних міст, але й важливою інфраструктурою та носієм послуг підтримки для підтримки ефективної координації міських цифрових урядів, високоякісного розвитку цифрової економіки, а також інклюзивного та гармонійного цифрового суспільства. З енергійним розвитком будівництва розумних міст різні інноваційні програми та послуги невіддільні від захисту та підтримки мережевої інфраструктури, такої як Інтернет та Інтернет речей, і пов'язані з цим проблеми мережевої безпеки стають все більш помітними, такі як перебої в обслуговуванні, атаки програм-вимагачів, витік інформації та інші проблеми, які спричинили величезні ризики та ризики безпеки для повсякденної роботи розумних міст.

Завдяки інноваціям концепції нагляду за кібербезпекою та прогресу регуляторних засобів, побудова аналізу ризиків безпеки, механізму спільного нагляду, технології інтелектуального нагляду та реагування на надзвичайні ситуації безпеки повинні координуватися та заохочуватися для супроводу розвитку розумних міст. загострилася гра в безпеку кіберпростору між великими державами. Російсько-український конфлікт поширив військові операції на кіберпростір, і Росія та Україна багато разів воювали одна з одною як сторони конфлікту. Під впливом російсько-українського конфлікту все більше країн посилюють нарощування кібервійськового потенціалу, наприклад, Сполучені Штати явно беруть наступальну кіберконцепцію за орієнтир і проводять різні форми кібероперацій, такі як передова оборона та передове полювання, що призводить до більшого виявлення ризиків для національної безпеки в кіберпросторі, що не лише посилює гру між усіма сторонами в процесі управління кіберпростором, але й змінює майбутнє порядку в кіберпросторі.

Ці ініціативи та практики вказують на те, як Європейський союз та країни Європи активно використовують цифрові технології для зміцнення соціально-економічної безпеки своїх громадян і підтримки сталого розвитку. Це включає в себе різноманітні політики, програми і дії, спрямовані на покращення економічної стабільності, забезпечення достатку населення, соціальної справедливості, охорони здоров'я, освіти, працевлаштування та інших аспектів життя суспільства.

Таблиця 9.6 – Європейські практики забезпечення соціально-економічної безпеки

Напрям забезпечення	Зміст та характеристика
Дигіталізація урядових послуг	Естонія виступає як лідер в електронному урядуванні, впроваджує концепцію «е-громадянина», де громадяни мають можливість здійснювати багато адміністративних послуг онлайн.
Цифрова трансформація	Цифрова інфраструктура, що включає розвиток технологій 5G та Інтернет речей (IoT), дозволяє покращити зв'язок та забезпечити ефективніше використання ресурсів в різних секторах економіки.
Фінтех та цифрові фінансові послуги,	Стартапи в області фінтеху в Європі: розвиток цифрових платіжних систем, фінансових технологій та блокчейн-технологій.
Цифрова Європа 2030	Цифрові інновації у виробництві та бізнесі включають Програму Європейського союзу «Цифрова Європа», яка спрямована на розвиток цифрових технологій у всіх сферах економіки.
Освіта та навчання: eTwinning та Erasmus+	Програми Європейського союзу для сприяння співпраці в галузі освіти та використання цифрових засобів для навчання та обміну досвідом.
Цифрові інструменти для забезпечення здоров'я	Електронна медична картка та телемедицина, використання цифрових рішень для поліпшення системи охорони здоров'я та доступу до медичних послуг.

Завдяки постійним інноваціям та глибокому застосуванню цифрових технологій, таких як хмарні обчислення та штучний інтелект, розумні міста також продемонстрували характеристики інтеграції, співпраці та інтелекту. Це стало новою тенденцією в розвитку розумних міст для кращого об'єднання послуг, людей і підприємств розумних міст через мережу. Основна цінність розумних міст полягає в досягненні високого ступеня централізації та обміну інформацією, але, сприяючи централізованому обміну інформаційними ресурсами, це також робить різні ризики безпеки більш концентрованими.

Хмарні обчислення, великі дані, Інтернет речей та мобільний інтернет породили нові вимоги до безпеки, які кардинально відрізняються від традиційного електронного урядування та традиційної інформатизації промисловості. На новому етапі розвитку розумні міста переходять від стаціонарних систем до систем чутливого стану, дані переходять від статичних до реальних часів, простор-час переходить від єдиних фізичних до багатовимірних соціальних мереж, а подальші межі мережевої безпеки поступово

узагальнюються та розмиваються, демонструючи характеристики легкої зміни, складності, неоднозначності та невизначеності, традиційний режим захисту кордонів, представлений брандмауерами та бастіонними господарями, поступово «дає збій», а традиційна архітектура безпеки, заснована на кордонах, більше не є надійною.

Традиційні методи захисту мережевої безпеки «виправлення», «часткове виправлення» та «після виправлення» більше не можуть задовольнити потреби майбутнього розвитку економічної та соціальної безпеки, а проектування мережевої безпеки на найвищому рівні з глобальної точки зору та систематичне розгортання стратегій мережевої безпеки та побудови інфраструктури на основі загального планування стануть основним напрямком розвитку мережевої безпеки в майбутньому.

Таблиця 9.7 – Основні заходи забезпечення соціально-економічної безпеки

Напрям забезпечення	Зміст та характеристика
Забезпечення стабільності національної економіки	Заходи для забезпечення стабільності національної економіки, контроль інфляції, підтримка фінансової системи.
Соціальне забезпечення	Системи соціального забезпечення, які забезпечують соціальні виплати, пенсії, допомогу безробітнім та інші форми підтримки для громадян.
Розвиток ринку праці	Розвиток ринку праці, стимулювання створення нових робочих місць, підтримка підприємництва.
Забезпечення якісної освіти	Забезпечення доступу до якісної освіти та медичних послуг, що сприяє зростанню людського капіталу та здоров'ю суспільства.
Розвиток соціальної справедливості	Розвиток соціальної справедливості, зменшення відмінностей в рівні доходів та можливостей.
Подолання економічних та соціальних криз	Розробка механізмів та стратегій для подолання економічних та соціальних криз, таких як фінансові кризи, епідемії тощо.

З розвитком інформаційних технологій стає все простіше прогнозувати тенденцію розвитку кібербезпеки, а також стає простіше використовувати величезну кількість інформації, наданої великими даними, для оцінки ризиків кібербезпеки, тому управління кібербезпекою є більш проактивним і більш ефективним і надійним. У зв'язку зі зростанням загроз і втрат, спричинених проблемами кібербезпеки, зростає попит на завчасне прогнозування та попереднє впровадження кібербезпеки, і необхідно продовжувати сприяти ітеративному оновленню технологій ризиків кібербезпеки, щоб сприяти проактивному управлінню кібербезпекою.

Глобальний механізм безпеки кіберпростору ще не сформований. У цифрову епоху інформаційні технології не лише принесли зручність у життя людей, а й створили умови для глобалізації та індустріалізації кіберзлочинності. На даному етапі світ стикається з серйозними викликами, такими як кібергегемонія, кіберзлочинність і витоки даних, які мають глибокий вплив на політичні, економічні, соціальні та культурні аспекти країн і регіонів. Три ключові сектори інфраструктури – фінанси, транспорт та енергетика – стали найбільш постраждалими сферами кібератак, а ситуація з безпекою є серйозною: 34 % кібератак відбувається у фінансовому секторі. З огляду на прихований і транснаціональний характер кіберзлочинності, що полегшує ухилення від нагляду, традиційний міжнародний механізм судової допомоги міжнародному кримінальному правосуддю має складні процедури, тривалі процеси та жорсткі умови, і вже не може відповідати потребам реальності. Однак прориву в розробці нових міжнародних правил для кіберпростору не відбулося.

Таблиця 9.8 – Концепції забезпечення соціально-економічної безпеки

Назва концепції	Автор і характеристкиа
Концепція економічної стабільності	Джон Мейнард Кейнс розглядав економічну стабільність та роль держави в регулюванні економіки.
Концепція соціального захисту	Бевері Пемслі – британськийо політик, який вплинув на створення системи соціального забезпечення у Великобританії після Другої світової війни.
Концепція зайнятості	Джон Гелбрейт розробив умови зайнятогсті у сфері економіки та ринку праці.
Концепція освіти та здоров'я	Амартія Сена внесла внесок у розвиток концепції людського розвитку, в якій освіта та здоров'я вважаються ключовими елементами.
Концепція соціальної солідарності	Жан-Жак Руссо розробив умови стосовно соціального контракту та солідарності.
Концепція кризового управління	Нассім Ніколас Талеб розробив концепцію управління ризиками у сучасному світі.
Концепції інновацій та розвитку	Джозеф Шумпетера аналізує процес творення нових інновацій та економічного розвитку.
Концепції, що відображають регіональні та міжнародні аспекти	Джозеф Стігліц аналізує проблеми глобалізації та соціальноекономічної справедливості, висуває ідеї щодо необхідності реформ у міжнародних економічних системах.
Концепції сучасних викликів та змін	Клаус Шваб висуває ідеї щодо змін у сучасному світі, такі як Четверта промислова революція та необхідність перегляду соціально-економічних систем.

Концепції забезпечення соціально-економічної безпеки можуть бути розглянуті з різних точок зору, оскільки включають мультидисциплінарний підхід. Крім того, різні країни можуть мати власні підходи до цієї теми, що відображається в їхніх національних стратегіях та політиках. Різні школи економічної та соціальної думки вносять свої внески у вирішення сучасних викликів та вдосконалення соціальних та економічних систем. В основі соцально-економічної безпеки – кібербезпека. Інструменти кібербезпеки мають цифровий інтелект. У міру того, як все більше і більше даних переміщується в хмару, питання кібербезпеки стають все більш складними.

Багато традиційних систем безпеки не можуть відстежувати дані хмарних обчислень, але нова кібербезпека на основі штучного інтелекту спеціально розроблена для хмарних обчислень, і впровадження гібридного рішення кібербезпеки, яке відстежує та аналізує дані в кількох операційних середовищах, стане необхідним заходом. З масовою популяризацією штучного інтелекту, включаючи нові технології, такі як Інтернет речей, генеруються величезні обсяги даних, і блокчейн може зіграти дуже хорошу роль у покращенні проблем шифрування, передачі, зберігання та захисту від несанкціонованого доступу цих даних.

Технологія блокчейн має вищу безпеку, ніж інші платформи або системи ведення записів, і будь-яка записана транзакція має бути узгоджена відповідно до правил консенсусу. Фальсифіковані докази та широко доступні реєстрації на основі блокчейну можуть забезпечити більшу прозорість та демократію даних. В даний час наша країна енергійно впроваджує різні політики для підтримки застосування та модернізації технології блокчейн. З 2020 року розвиток глобальної цифрової економіки значно прискорився, завдяки побудові «нової інфраструктури», представленої 5G та блокчейном, що розгортається всебічно, а також глибокій інтеграції блокчейну з передовими технологіями, такими як Інтернет речей, великі дані, хмарні обчислення та штучний інтелект.

Необхідні сформувати умови для модернізації системи та спроможностей національної безпеки. По-перше, побудова міцної лінії оборони для кібербезпеки пов'язана з національною безпекою та соціальною стабільністю. У сучасну епоху зміст і форма стратегічних ігор і боротьби за безпеку в кіберпросторі стали більш складними, і необхідно терміново побудувати міцну лінію захисту для кібербезпеки. Кіберпростір став не лише першим полем бою для різних кібератак та загроз безпеці, а й важливим полем для сприяння соціальному управлінню. По-друге, мережева безпека є необхідною умовою злагодженого розвитку інформатизації. Як історична концепція, що постійно розвивається, основні вимоги «модернізації» зазнали

ключової трансформації від індустріалізації до інформатизації. З популяризацією та застосуванням інформаційних технологій акцент модернізації поступово змістився на сферу інформаційних технологій. Мережева безпека та інформатизація – це два крила одного корпусу та два колеса приводу. Інформатизація надає сприятливу можливість розвивати командні висоти нового витка розвитку і створити нові переваги в міжнародній конкуренції, що вимагає єдиного планування і розгортання. Мережева безпека дає сильну гарантію для злагодженого розвитку інформатизації.

Таким чином, аналіз діджиталізації дозволяє зрозуміти, які сучасні технології використовуються для покращення соціально-економічної безпеки. Вивчення практик діджиталізації сприяє розвитку теоретичних концепцій щодо того, як ці технології можуть впливати на соціальні та економічні аспекти суспільства. Тема дозволяє глибше розуміти, як впровадження цифрових інструментів впливає на взаємодію між людьми та інституціями. Використання європейських практик діджиталізації може допомогти покращити ефективність управління різними галузями економіки та соціальними послугами. Зростання цифровизації може призвести до нових викликів у сфері кібербезпеки, вивчення європейських практик допомагає розробити стратегії та заходи забезпечення безпеки в цифровому середовищі. Перенесення європейських практик діджиталізації може сприяти створенню інноваційних рішень у сфері економіки, соціального захисту та інших галузях. Цифрові технології можуть полегшити доступ до інформації та ресурсів, що сприяє соціальній інклюзії та покращенню рівня життя. Впровадження цифрових інновацій може підвищити конкурентоспроможність країни на міжнародному ринку. Комплексний аналіз засвідчив, що тема не лише важлива для теоретичного розвитку науки, але й має практичне застосування у вдосконаленні соціально-економічних процесів у сучасному суспільстві для забезпечення стабільності та захисту інтересів держави воєнного і поствоєнного розвитку. Наведені найкращі практики та технології можуть допомогти організації створити надійну кібербезпеку, яка зменшить вашу вразливість до кібератак і захистить критично важливі інформаційні системи, не впливаючи на взаємодію з користувачем або клієнтом.

9.2 ЦИФРОВА БЕЗПЕКА

З бурхливим розвитком інформаційних технологій все частіше з'являються такі терміни, як мережева безпека, інформаційна безпека та безпека даних, що є різновидами цифрової бехпеки і становлять систему мережевої безпеки. Насправді є багато людей, які не в змозі

відрізнити поняття мережева безпека, інформаційна безпека та безпека даних. Мережева безпека запобігає несанкціонованому доступу до мережевих ресурсів, а також допомагає виявляти та припиняти поточні кібератаки та порушення мережевої безпеки. У той же час мережева безпека допомагає забезпечити авторизованим користувачам безпечний і швидкий доступ до потрібних їм мережевих ресурсів.

Мета роботи – теоретичні і практичні аспекти дослідження системи безпеки (інформаційної, цифрової, мережевої) як чинник забезпечення цілісності кіберпростору.

Матеріали та методи. Використання міждисциплінарного підходу з використанням методів філософії, кібернетики, програмування, що дозволили здійснити цілісне дослідження складної теми в умовах викликів цифровізації, глобалізації, Четвертої промислової революції. В основі міждисциплінарного підходу аналіз різних систем мережевої безпеки, мережевого трафіку для виявлення та оцінки загроз, використання симуляційних моделей для аналізу ефективності різних методів мережевої безпеки, розробка сценаріїв можливих атак і перевірка захисних заходів, аналіз конкретних випадків успішного захисту та порушення безпеки, вивчення найкращих практик та стратегій управління мережею у великих організаціях, використання статистичних методів для оцінки ефективності різних систем та методів захисту, аналіз ризиків і вразливостей мережевих систем.

Цифрова безпека відіграє ключову роль у захисті організацій від кіберзагроз, має вирішальне значення для захисту мережі організації від несанкціонованого доступу чи атак, для захисту програм та систем організації від несанкціонованого доступу або атак. Цифрова безпека має широкий спектр застосувань у всіх сферах життя. Наприклад, у сфері охорони здоров'я цифрова безпека має вирішальне значення для захисту інформації про пацієнтів та забезпечення конфіденційності та безпеки електронних медичних записів. У фінансовій галузі цифрова безпека має вирішальне значення для захисту конфіденційної фінансової інформації та забезпечення цілісності фінансових транзакцій. У сфері роздрібної торгівлі цифрова безпека має вирішальне значення для захисту інформації про клієнтів та забезпечення безпеки онлайн-транзакцій.

Важливо відзначити, що цифрова безпека – це область, що постійно розвивається, і фахівці в цій галузі повинні бути в курсі новітніх загроз і технологій, щоб працювати ефективно. Цифрова безпека – це комплекс заходів і практик, спрямованих на захист цифрових активів, інформації та технологій від різноманітних загроз у кіберпросторі. Це включає захист від кібератак, захист конфіденційності даних, забезпечення безпеки онлайн-транзакцій, а також захист від втручання в цифрову інфраструктуру.

Таблиця 9.9 – Основні напрями захисту цифрової безпеки

Напрямок	Зміст і характеристика
Захист даних	Забезпечення безпеки даних, як у процесі їх зберігання, так і під час передачі, щоб уникнути їх несанкціонованого доступу або розголошення. Це досягається за допомогою шифрування, резервного копіювання та політик управління даними.
Захист пристроїв	Гарантування безпеки цифрових пристроїв, таких як комп'ютери, смартфони, планшети, які можуть бути вразливими до вірусів, шкідливого ПЗ, фішинг-атак та інших загроз.
Кібергігієна	Практика відповідального користування цифровими пристроями та інтернетом. Це включає в себе регулярне оновлення програмного забезпечення, використання складних паролів, активацію двофакторної аутентифікації та уникнення підозрілих посилань.
Інформаційна обізнаність	Освіта користувачів щодо можливих загроз у кіберпросторі, таких як фішинг, зломи або викрадення особистих даних, і надання їм знань про те, як захистити себе.
Захист мережі	Забезпечення безпеки мережевих інфраструктур, включаючи домашні та корпоративні мережі. Це включає налаштування брандмауерів, використання VPN для захищеного доступу до мережі, та моніторинг активності для виявлення аномалій.
Безпека програмного забезпечення	Розробка і використання безпечного програмного забезпечення, яке не містить вразливостей, що можуть бути використані зловмисниками. Це включає регулярне оновлення та виправлення програмного забезпечення.
Захист особистих даних	Забезпечення конфіденційності особистих даних користувачів та дотримання законодавчих вимог щодо їх обробки та зберігання, таких як GDPR.

Цифрова безпека охоплює ширший спектр захисту, ніж просто мережева або інформаційна безпека, оскільки включає в себе також захист особистих пристроїв, онлайн-активностей і приватності користувачів. Вона стосується не тільки організаційних, але й особистих аспектів безпеки, оскільки кожен користувач цифрових технологій повинен дбати про свою власну безпеку в інтернеті. У сучасному світі, де цифрові технології стали невід'ємною частиною життя, захист від кіберзагроз є критично важливим. Це стосується як приватних осіб, так і великих організацій, які стикаються з ризиками, пов'язаними з втратою даних, кібератаками, порушенням конфіденційності тощо. Цифрова безпека допомагає мінімізувати ці ризики, захищаючи особисту інформацію, фінансові дані та інші цифрові активи від загроз.

Інформаційна безпека охоплює всі заходи, що забезпечують захист інформації від різноманітних загроз, незалежно від форми, в якій ця інформація зберігається або передається (цифрова, фізична, усна). Основна мета

інформаційної безпеки – зберегти три основні характеристики інформації, вона охоплює широкий спектр заходів, включаючи фізичну безпеку, політику доступу, управління ризиками, аудит та інші управлінські та технічні заходи.

Інформаційна безпека це галузь, що займається захистом інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, модифікації, знищення або порушення доступності. Метою інформаційної безпеки є забезпечення трьох ключових аспектів: 1) Конфіденційність (Confidentiality), яка націлена на забезпечення того, щоб доступ до інформації мали тільки авторизовані особи або системи. Це досягається через використання шифрування, контроль доступу та інші методи захисту даних. 2) Цілісність (Integrity), в основі якої гарантування того, що інформація залишається незмінною та точною, і не була змінена або пошкоджена несанкціонованими особами. Для цього використовуються методи, такі як контроль версій, цифрові підписи та контрольні суми. 3) Доступність (Availability), в основі якої забезпечення того, що інформація та системи доступні для використання в потрібний час. Це включає захист від атак типу «відмова в обслуговуванні» (DDoS), резервне копіювання даних та аварійне відновлення. Інформаційна безпека є найширшим терміном, який включає всі аспекти захисту інформації незалежно від її форми та середовища.

Таблиця 9.10 – Основні компоненти інформаційної безпеки

Компонент	Зміст і характеристика
Керування доступом	Встановлення політик і процедур для управління доступом до інформації та систем, включаючи паролі, біометричні дані та інші механізми аутентифікації.
Шифрування	Перетворення інформації в код, який можна прочитати лише за допомогою ключа розшифрування. Це важливо для захисту конфіденційних даних під час їх передачі або зберігання.
Політика безпеки	Набір правил і процедур, що визначають, як інформація повинна бути захищена в організації. Політика включає правила щодо паролів, управління доступом, використання мобільних пристроїв та інших аспектів безпеки.
Моніторинг та аудит	Постійне відстеження та аналіз активності в системах для виявлення та запобігання загрозам. Аудит дозволяє перевіряти, чи дотримуються політики безпеки і чи немає порушень.
Навчання та підвищення обізнаності	Інформаційна безпека значною мірою залежить від поведінки користувачів, тому навчання співробітників і користувачів є ключовим для зниження ризику людських помилок.
Інцидент-менеджмент	Процедури для реагування на порушення безпеки або інциденти, такі як зломи, вірусні атаки або втрати даних. Це включає виявлення, реагування, усунення наслідків та аналіз інциденту.

Інформаційна безпека є критично важливою в сучасному цифровому світі, де дані стали одним із найцінніших активів. Захист інформації забезпечує довіру, зберігає репутацію компаній та організацій, а також захищає особисту інформацію користувачів. Інформаційна безпека формується у контексті забезпечення конфіденційності, цілісності, доступності та достовірності інформації. З точки зору визначення, не існує суворого стандартного визначення інформаційної безпеки, але з урахуванням контенту, що займається інформаційною безпекою, інформаційна безпека гарантує, що інформація, яка зберігається або передається, не може бути навмисно або ненавмисно вкрадена і знищена іншими особами. «Інформація» тут включає в себе широкий спектр контенту, такий як «звук», «дані», «біометрія» і так далі. Як випливає з назви, інформаційна безпека в основному зосереджена на безпеці самої інформації. Інформаційна безпека ґрунтується на основних атрибутах – конфіденційності, цілісності та доступності інформації та доповнюється розширеними атрибутами, такими як незаперечення (anti-repudiation), автентичність та контрольованість. Значення інформаційної безпеки полягає в захисті безпеки самої інформації і безпеки носія інформації, тобто інформаційної системи.

Основне призначення комп'ютерної мережі полягає в забезпеченні зв'язку між різними комп'ютерними пристроями для обміну даними, спільного використання ресурсів та забезпечення централізованого управління і доступу до інформації. Комп'ютерні мережі дозволяють кільком користувачам взаємодіяти між собою та використовувати спільні ресурси, такі як файли, принтери, бази даних, програмне забезпечення, інтернет-доступ та інші послуги.

Основні функції комп'ютерної мережі: 1) Мережа дозволяє користувачам передавати файли, документи, повідомлення та іншу інформацію між комп'ютерами. 2) Користувачі можуть спільно використовувати периферійні пристрої, такі як принтери, сканери та накопичувачі даних, що дозволяє знижувати витрати на обладнання. 3) Мережі дозволяють зберігати дані та програмне забезпечення на серверах, до яких можуть звертатися користувачі з різних пристроїв, забезпечуючи централізоване управління. 4) Завдяки мережам можлива організація спільної роботи над проектами, що дозволяє групам співробітників співпрацювати та обмінюватися інформацією в режимі реального часу. 5) Мережі дозволяють адміністраторам централізовано управляти доступом до ресурсів, а також забезпечувати безпеку даних через політики доступу, резервне копіювання, шифрування та інші заходи. 6) Комп'ютерні мережі забезпечують підключення до інтернету, що дозволяє користувачам обмінюватися інформацією з зовнішніми ресурсами та взаємодіяти з глобальними інформаційними

системами. Комп'ютерні мережі є основою сучасної інформаційної інфраструктури, забезпечуючи можливість ефективного обміну інформацією, спільного використання ресурсів та централізованого управління, що є критично важливим для успішної роботи як невеликих організацій, так і великих корпорацій. Основне призначення комп'ютерної мережі полягає в спільному використанні ресурсів, так як мережа зв'язку – це спосіб реалізації спільного використання мережевих ресурсів. Комп'ютерна мережа безпечна, відповідна комп'ютерна комунікаційна мережа також повинна бути безпечною, повинна мати можливість здійснювати обмін інформацією та спільне використання ресурсів для користувачів мережі.

Мережева система не схильна до будь-яких загроз і посягань і, як правило, може реалізовувати функцію спільного використання ресурсів. Для того, щоб в мережі нормально реалізовувалася функція спільного використання ресурсів, необхідно забезпечити нормальну роботу апаратного і програмного забезпечення мережі, а потім забезпечити безпеку обміну даними та інформацією. **Поняття мережевої безпеки** необхідно аналізувати її в поєднанні з ситуацією, якщо «мережева безпека» протиставляється «безпеці системи», «безпеці додатків», «безпеці даних». Під мережевою безпекою маються на увазі проблеми безпеки, викликані необхідністю функціонування елементів інформаційної системи через Інтернет у вузькому сенсі. Однак, коли говорять про кібербезпеку, зазвичай мають на увазі безпеку інформаційних систем та інформації в кіберпросторі, тобто «безпеку кіберпростору» також називають кібербезпекою. Оскільки найважливішою формою носія інформаційної системи є Інтернет, мережева безпека часто використовується для позначення інформаційної безпеки. **Інформаційна безпека і цифрова безпека** є взаємопов'язаними поняттями, але вони мають різні акценти та охоплюють дещо різні аспекти захисту в кіберпросторі.

Таблиця 9.11 – Ключові відмінності між інформаційною та цифровою безпекою

Інформаційна безпека	Цифрова безпека
1	2
Зосереджується на захисті інформації в будь-якій формі, будь то цифрова, фізична, друкована або інша. Вона включає заходи для захисту конфіденційності, цілісності та доступності даних. Інформаційна безпека охоплює як цифрову інформацію, так і інформацію на паперових носіях або в розмовній формі.	Вужчий термін, що стосується захисту конкретно цифрових активів та інформації, яка зберігається, обробляється або передається в цифровому вигляді. Вона включає захист цифрових пристроїв, мереж, онлайн-активностей та персональних даних користувачів у цифровому середовищі.

Закінчення таблиці 9.11

1	2
Захищає всю інформацію незалежно від її форми чи носія. Це може включати як цифрові дані, так і фізичні документи, що містять конфіденційну інформацію. Також це включає управління доступом до інформації, незалежно від того, як вона зберігається або передається.	Охоплює виключно цифрові об'єкти, такі як файли, бази даних, цифрові пристрої (комп'ютери, смартфони), мережі, програмне забезпечення та інтернет-активності. Основна увага приділяється захисту від кіберзагроз, які стосуються цифрового світу.
Включає широкий спектр методів захисту, таких як фізична безпека (захист будівель, серверних кімнат), адміністративні заходи (політики, процедури), а також технічні засоби (шифрування, брандмауери). Вона також враховує управління ризиками, аудит і контроль відповідності законодавчим нормам.	Сфокусована на технічних заходах захисту в цифровому середовищі. Це включає шифрування даних, антивірусне програмне забезпечення, кібергігієну, захист цифрових пристроїв і мереж, управління доступом до цифрових ресурсів, захист від фішинг-атак та інші заходи, що забезпечують безпеку в онлайн-просторі.
Застосовується у всіх сферах діяльності, де обробляється інформація. Це може включати як бізнес, урядові установи, так і особисте життя, де важливо захистити будь-яку інформацію від несанкціонованого доступу чи втрат.	Більше стосується сучасних цифрових технологій і використовується там, де є потреба в захисті інформації в інтернеті, на цифрових пристроях і в хмарних середовищах. Це актуально для користувачів інтернету, компаній, що використовують цифрові платформи, та тих, хто зберігає інформацію в цифровому вигляді.
Інформаційна безпека є ширшим поняттям і охоплює захист усіх видів інформації, незалежно від форми	Цифрова безпека зосереджена виключно на захисті інформації та активів у цифровому середовищі.

Обидві сфери є важливими в контексті захисту даних, але їхня специфіка та методи можуть відрізнятися залежно від середовища та типу інформації, що захищається.

Мережева безпека включає в себе інформаційну безпеку і безпеку даних. Деякі вважають, що між ними існує взаємний зв'язок, наприклад, кібербезпека, інформаційна безпека, дорівнює безпеці даних. Насправді кожен із цих видів безпеки представляє свої власні поля та акценти, проте є відмінності та спільні риси. Мережева безпека ґрунтується на положенні мережі як основної системи безпеки, в основному із залученням доменів мережевої безпеки, брандмауерів, контролю доступу до мережі, анти-DDOS та інших сценаріїв, а ще мається на увазі оточення всього кіберпростору. Мережева інформація та дані можуть існувати як у кіберпросторі, так і поза кіберпростором. «Дані» можна розглядати як основний

носій «інформації», а інформація є цінним активом, який робить осмислений аналіз даних. З іншого боку, безпека даних орієнтована на дані, зосереджуючись на безпеці та відповідності циклу безпеки даних, щоб захистити безпеку даних. Поширені інциденти безпеки даних включають витік даних і фальсифікацію даних. Мережева безпека (або кібербезпека) – це практика захисту комп'ютерних мереж від різних загроз, що можуть завдати шкоди або порушити конфіденційність, цілісність, і доступність інформації.

Таблиця 9.12 – Основні аспекти мережевої безпеки

Аспект	Зміст і характеристика
Аутентифікація та авторизація	Визначення та перевірка користувачів і пристроїв, щоб гарантувати, що доступ до мережі надається лише тим, хто має відповідні права.
Шифрування	Захист інформації шляхом її перетворення у код, який може бути прочитаний лише авторизованими користувачами.
Захист від шкідливого ПЗ (малвару)	Виявлення і запобігання проникненню вірусів, троянів, шпигунських програм та інших видів шкідливого ПЗ.
Мережева сегментація	Розподіл мережі на менші, ізольовані сегменти для обмеження поширення шкідливих програм і несанкціонованого доступу.
Системи виявлення та запобігання вторгнень (IDS/IPS)	Моніторинг мережі для виявлення та запобігання підозрілим активностям.
Брандмауери	Програмні або апаратні засоби, які контролюють і фільтрують вхідний та вихідний трафік на основі певних правил.
VPN (Virtual Private Network)	Технологія, яка дозволяє створювати захищені, шифровані з'єднання між користувачами та мережами, навіть через відкритий Інтернет.
Оновлення та патчинг	Регулярне оновлення програмного забезпечення, застосування патчів для виправлення вразливостей.
Брандмауери (файрволи)	Контроль трафіку між різними частинами мережі.
Системи виявлення та запобігання вторгнень (IDS/IPS):	Виявлення і запобігання підозрілим активностям у мережі.

Мережева безпека є критично важливою для захисту конфіденційної інформації, забезпечення безперервності бізнесу та запобігання витоку даних. Мережева безпека та хмарна безпека є взаємопов'язаними, але вони мають різні акценти та підходи. Мережева безпека фокусується на захисті локальних або глобальних мереж організації від різноманітних загроз. Це включає захист фізичних і віртуальних мережевих інфраструктур, таких як маршрутизатори, комутатори, сервери та інші пристрої, що забезпечують роботу мережі.

Хмарна безпека захищає хмарні активи та сервіси організацій: програми, дані, сховища, інструменти розробника, віртуальні сервери та хмарну інфраструктуру. Загалом, хмарна безпека працює за моделлю спільної відповідальності, в якій постачальник хмарних послуг відповідає за безпеку послуг, які він надає, та інфраструктури, що використовується для їх надання. Клієнт несе відповідальність за захист даних, коду та інших активів, які він зберігає або використовує в хмарі. Деталі різняться залежно від використовуваних хмарних сервісів. **Хмарна безпека** стосується захисту даних, програм та інфраструктури, що розміщені в хмарних середовищах (наприклад, Amazon Web Services (AWS), Microsoft Azure, Google Cloud). Оскільки хмарні сервіси передбачають віддалене зберігання та обробку даних, хмарна безпека зосереджується на захисті цих даних і ресурсів від несанкціонованого доступу, збоїв, втрат та інших загроз.

Основні аспекти хмарної безпеки включають: 1) Управління правами доступу до хмарних ресурсів. 2) Захист даних під час їх зберігання та передачі. 3) Забезпечення безпеки інтерфейсів прикладного програмування (API), які використовуються для взаємодії з хмарними сервісами. 4) Постійне відстеження активності в хмарі для виявлення аномалій або загроз. 5) Дотримання стандартів та норм безпеки, таких як GDPR, PCI DSS тощо.

Основні відмінності між мережевою і хмарною безпекою: 1) Місце розташування: якщо мережева безпека охоплює захист локальних і глобальних мереж, тоді як хмарна безпека зосереджена на захисті ресурсів, розміщених у хмарі. 2) Інфраструктура: якщо мережева безпека включає захист фізичної мережевої інфраструктури, то хмарна безпека більше фокусується на віртуальних середовищах та віддалених даних. 3) Підходи до управління: хмарна безпека часто вимагає спеціальних підходів до управління доступом і захистом даних, враховуючи, що ресурси можуть бути доступні через Інтернет. Таким чином, мережеву безпеку і хмарну безпеку можна розглядати як окремі, але взаємодоповнюючі сфери кібербезпеки, кожна з яких має свої особливості та виклики.

Безпека даних. Дані є носієм інформації, існуванням систем введення і виведення інформації. Типові форми даних включають бази даних, документи, зображення, структуровані/неструктуровані форми тощо. Ядро захисту інформаційної безпеки орієнтоване на дані, а його основна концепція полягає в забезпеченні нормального використання даних бізнес-системами. Визначення безпеки даних є відносно специфічним. Під даними мається на увазі будь-який запис інформації, як в електронному вигляді, так і в іншому вигляді. Обробка даних включає збір, зберігання, використання,

обробку, передачу, надання та розкриття даних. Безпека даних означає вжиття необхідних заходів для забезпечення того, щоб дані перебували в стані ефективного захисту та законного використання, а також мали можливість забезпечувати безперервний стан безпеки. Концепція безпеки даних більш конкретна та інтуїтивно зрозуміла, ніж кібербезпека та інформаційна безпека.

Традиційні моделі захисту периметра мережі не підходять для захисту хмарної інфраструктури, і потрібні нові підходи. Для цього потрібні комплексні інструменти виявлення та класифікації хмарних даних, а також постійний моніторинг активності та управління ризиками. Інструменти хмарного моніторингу можуть бути розгорнуті між рішеннями бази даних як послуга (DBaaS) постачальників хмарних послуг для моніторингу транзитних даних або перенаправлення трафіку на існуючу платформу безпеки підприємства. Таким чином, політики можуть застосовуватись однаково незалежно від того, де знаходяться дані.

Використання ПК, планшетів та мобільних пристроїв у корпоративних обчислювальних середовищах продовжує зростати, але керівники служб безпеки стурбовані ризиками, пов'язаними з цією практикою. Один із способів покращити безпеку використання власних пристроїв (BYOD) – вимагати від співробітників, які приносять свої власні пристрої, встановлювати програмне забезпечення безпеки перед доступом до корпоративної мережі, підвищуючи централізований контроль над доступом до даних та їх переміщенням, а також зміцнюючи весь процес. візуальний менеджмент. Інша стратегія полягає в розповсюдженні інформації про безпеку на підприємстві, заохочення співробітників до використання важкозламуваних паролів, багатофакторної автентифікації, регулярного оновлення програмного забезпечення, а також навчання резервного копіювання пристроїв та шифрування даних у рамках цих тренінгів тощо.

Завдяки спільним зусиллям усіх верств суспільства система безпеки даних стає дедалі досконалішою. Однак для створення комплексної та тривимірної системи забезпечення безпеки даних, окрім політичних та інституційних гарантій, також потрібно, щоб відповідні суб'єкти ринку підвищували свою обізнаність та робили запобіжні дії, прискорювали побудову системи безпеки, яка була б як внутрішньою, так і зовнішньою. Потреби безпеки є однією з основних потреб людини. Коли справа доходить до захисту інформації користувачів та особистого життя, компанії повинні ефективно виконувати свої соціальні обов'язки, щоб користувачі могли відчувати себе у більшій безпеці.

Щоб ефективно захистити цифрову безпеку, необхідно реалізувати класифікацію даних та ієрархічне управління, наукове сортування активів даних, точно ідентифікувати важливі дані та основні дані, встановити

допоміжну класифікацію та ієрархічне управління. з іншого боку, ефективний механізм, активно розвивати підготовку спеціалістів у галузі цифрової безпеки, створювати талановиту команду з сильними технічними можливостями та високим професіоналізмом, створювати неприступну «систему цифрової безпеки» за допомогою органічного співробітництва та взаємного доповнення між цифровою безпекою, співробітниками та якісними цифровими системами безпеки.

Таким чином, інформаційна безпека, кібербезпека та безпека даних, хоча всі вони є поняттями, пов'язаними з інформаційною безпекою, зосереджені на дещо різних об'єктах та сферах. На практиці потрібно вжити відповідних заходів безпеки для забезпечення інформаційної безпеки, мережевої безпеки та безпеки даних відповідно до конкретної ситуації, щоб гарантувати, що наше життя в Інтернеті буде безпечним і стабільним. Стрімкий розвиток нових технологій і додатків, таких як цифрова економіка, інтернет-фінанси, штучний інтелект, великі дані та хмарні обчислення, породив низку нових форм і моделей, але все ще існують часові лаги та білі області у відповідних правових системах. **Інформаційна безпека**, **кібербезпека**, і **безпека даних** – це взаємопов'язані, але різні поняття, які стосуються захисту інформації та систем. Кожне з них має свої специфічні аспекти і завдання (табл. 9.13).

Кожна з цих сфер є важливою складовою загальної стратегії захисту інформації в сучасному світі, де цифрові технології відіграють ключову роль у житті суспільства та бізнесу (табл. 9.14).

Основні заходи безпеки даних є необхідними, тому що мають місце загрози, з якими організації та підприємства повинні боротися: 1) Кіберзлочинність, так як процвітають хакерські атаки, фішинг, зломи, викрадення даних або програми-здирники, що загрожують конфіденційності та цілісності даних. 2) Витоки даних можуть статися через людський фактор (наприклад, помилки персоналу), помилки в програмному забезпеченні або зловмисні дії. 3) Втрата даних через збої в системах, аварії або природні катастрофи, що можуть призвести до незворотних втрат інформації. 4) Внутрішні загрози включають зловмисні дії співробітників або партнерів, які мають доступ до конфіденційних даних. Захист даних є критично важливим у сучасному цифровому світі, тому що дані – це не лише інформація про клієнтів, фінансові операції чи комерційні таємниці, але й особисті дані користувачів, які є надзвичайно цінними для будь-якої організації. Втрата або компрометація даних може призвести до серйозних фінансових втрат, пошкодження репутації та юридичних наслідків. Тому безпека даних є ключовим аспектом для будь-якої організації, що прагне захистити свою інформацію та забезпечити довіру клієнтів і партнерів.

Таблиця 9.13 – Основні завдання кібербезпеки і безпеки даних

Кібербезпека	Завдання	Безпека даних	Завдання
Кібербезпека є підмножиною інформаційної безпеки і зосереджується на захисті комп'ютерних систем, мереж та даних від кіберзагроз, які виникають у кіберпросторі. Це поняття охоплює всі аспекти безпеки, пов'язані з використанням інтернету та цифрових технологій.	Основні завдання кібербезпеки включають: захист від кібератак, таких як хакерські атаки, фішинг, DDoS-атаки; захист мережевої інфраструктури, серверів, комп'ютерів, мобільних пристроїв та програмного забезпечення; реагування на інциденти кібербезпеки та їх усунення.	**Безпека даних є специфічним аспектом як і**нформаційної, так і кібербезпеки. Вона стосується захисту даних, незалежно від того, де і як вони зберігаються або передаються. Це може включати як структуровані дані (наприклад, бази даних), так і неструктуровані дані (наприклад, текстові файли, електронні листи).	Основні завдання безпеки даних включають: шифрування, що включає перетворення даних у форму, яку можуть прочитати лише авторизовані особи або системи Створення копій даних для відновлення у разі втрати або пошкодження оригіналу. Контроль доступу: визначення, хто має право доступу до певних даних і на яких умовах.
Кібербезпека охоплює як технічні аспекти, так і освітні заходи, що спрямовані на підвищення обізнаності користувачів про можливі загрози. Кібербезпека фокусується на захисті цифрових інформаційних систем і мереж від загроз, що виникають в кіберпросторі.	Моніторинг мережевої активності для виявлення та запобігання загрозам. звиток інтегрованих систем, об'єднуючи фізичні та кібернетичні складники.	Безпека даних – це комплекс заходів, стратегій і технологій, спрямованих на захист даних від несанкціонованого доступу, викрадення, пошкодження або втрати. Вона охоплює різноманітні аспекти захисту інформації, яка може бути як в електронному, так і в фізичному вигляді.	Захист від втрати даних (DLP): технології та політики, що запобігають несанкціонованій передачі або витоку даних за межі організації. Анонімізація та маскування даних: техніки, що захищають конфіденційні дані, приховуючи або змінюючи ідентифікатори. Безпека даних зосереджується на конкретних заходах для захисту даних, як цифрових, так і фізичних, включаючи їх зберігання, обробку та передачу.

Таблиця 9.14 – Основні заходи безпеки даних

Заходи	Зміст і характеристика
Шифрування	Один із найефективніших методів захисту даних, що перетворює інформацію в закодовану форму, доступну лише тим, хто має ключ для розшифрування.
Резервне копіювання даних	Створення копій даних на випадок їх втрати або пошкодження. Це дозволяє відновити інформацію з резервних копій у разі надзвичайної ситуації.
Контроль доступу	Впровадження систем, що обмежують доступ до даних лише авторизованим користувачам. Це може включати такі механізми, як багатофакторна аутентифікація (MFA) та рольовий доступ (RBAC).
Аудит та моніторинг	Постійне відстеження доступу до даних і використання ресурсів для виявлення потенційних загроз або аномальної активності.
Захист від втрати даних (DLP)	Технології, які запобігають несанкціонованій передачі конфіденційної інформації за межі організації, що дозволяє уникнути витоків даних.
Анонімізація та маскування даних	Методи захисту конфіденційної інформації, що передбачають зміну або видалення ідентифікаційних даних, щоб зробити їх менш доступними для зловмисників.
Політики безпеки	Розробка та впровадження чітких правил і процедур щодо обробки, зберігання та передачі даних. Це включає інструкції щодо використання паролів, управління доступом, обробки конфіденційної інформації тощо.

Безпека додатків – це заходи, що вживаються командами безпеки для захисту програм та інтерфейсів прикладного програмування (API) від кібератак.

Сьогодні багато компаній використовують програми для виконання критично важливих для бізнесу функцій або обробки конфіденційних даних, програми є поширеною мішенню для кіберзлочинців. А оскільки так багато бізнес-додатків розміщено в загальнодоступній хмарі, хакери можуть використовувати їхні вразливості для злому корпоративних приватних мереж. Заходи безпеки додатків захищають програми від зловмисників. **Безпека додатків** (або **аплікаційна безпека**) – це набір практик, технологій та заходів, спрямованих на захист програмного забезпечення від загроз, вразливостей та атак на всіх етапах його розробки, впровадження та використання. Основною метою безпеки додатків є забезпечення того, щоб програми працювали відповідно до вимог безпеки і не піддавалися ризику з боку зловмисників.

Таблиця 9.15 – Ключові аспекти безпеки додатків

Заходи	Зміст і характеристика
Безпечне програмування	Дотримання принципів безпечного програмування, таких як валідація вводу, захист від ін'єкцій SQL, управління пам'яттю та уникнення використання небезпечних функцій.
Статичний аналіз коду	Використання інструментів для аналізу вихідного коду на предмет вразливостей ще на етапі розробки.
Дизайн з урахуванням безпеки	Впровадження безпечної архітектури додатку, яка враховує потенційні загрози та ризики.
Захист на рівні архітектури	Аналіз архітектури додатка для ідентифікації потенційних загроз і розробка відповідних заходів захисту.
Аутентифікація та авторизація	Забезпечення, що лише авторизовані користувачі мають доступ до певних функцій або даних у додатку.
Рольовий доступ	Визначення та управління ролями користувачів для обмеження доступу до критичних функцій або даних.
Шифрування	Використання шифрування для захисту конфіденційних даних як під час їх передачі, так і зберігання.
Інтеграція безпеки у SDLC	Залучення практик безпеки на всіх етапах розробки програмного забезпечення, починаючи з планування, дизайну, тестування і до розгортання.
DevSecOps	Інтеграція безпеки в процеси DevOps, що забезпечує автоматизацію безпекових перевірок на всіх етапах розробки та експлуатації додатків.
Захист від ін'єкцій	Запобігання атакам типу SQL-ін'єкцій, XSS (міжсайтовий скриптинг), CSRF (підробка міжсайтових запитів) тощо.
WAF (Web Application Firewall)	Використання брандмауерів для веб-додатків, які забезпечують захист від відомих атак на веб-додатки.
Динамічний аналіз	Аналіз поведінки додатку під час його виконання для виявлення потенційних вразливостей, які можуть проявитися лише під час роботи.
Оновлення безпеки	Регулярне застосування оновлень безпеки для усунення вразливостей.
Управління патчами	Впровадження процесу швидкого розгортання патчів для мінімізації ризику експлуатації відомих вразливостей.
Навчання розробників	Підвищення обізнаності розробників про найкращі практики безпеки та найпоширеніші вразливості.
Інструктаж користувачів	Навчання користувачів безпечному використанню додатків, включаючи управління паролями та розпізнавання фішингових атак.

У сучасному світі додатки, особливо веб- і мобільні додатки, є основними інструментами для доступу до даних і взаємодії з користувачами. Вразливості в додатках можуть призвести до серйозних наслідків, таких

як витік конфіденційних даних, фінансові втрати, порушення роботи сервісів або навіть компрометація всієї інформаційної системи. Тому безпека додатків є критично важливою складовою загальної безпеки організації та потребує постійного вдосконалення і адаптації до нових загроз і технологічних змін.

Поширені інструменти безпеки додатків включають брандмауери веб-додатків, самозахист додатків під час виконання, статичне тестування безпеки додатків і динамічне тестування безпеки додатків. За результатамии індексу IBM Security X-Force Threat Intelligence Index, фішингє найпоширенішим початковим вектором кібератаки. Інструменти безпеки електронної пошти можуть допомогти зупинити фішингові атаки та інші спроби скомпрометувати облікові записи електронної пошти користувачів. Більшість поштових сервісів мають вбудовані інструменти безпеки, такі як фільтри спаму та шифрування повідомлень. Деякі інструменти захисту електронної пошти постачаються з ізольованим програмним середовищем, і в таких ізольованих середовищах команди безпеки можуть перевіряти вкладення електронної пошти на наявність шкідливого програмного забезпечення.

Захист від втрати даних – це політики та інструменти інформаційної безпеки, які гарантують, що конфіденційні дані не будуть викрадені або випадково витоку. DLP включає політики безпеки даних і спеціально розроблені технології, які можна використовувати для відстеження потоків даних, шифрування конфіденційної інформації та оповіщення про виявлення підозрілої активності. Рішення для захисту кінцевих точок захищають будь-який пристрій, підключений до вашої мережі, наприклад ноутбуки, настільні комп'ютери, сервери, мобільні пристрої або пристрої IoT, запобігаючи спробам хакерів використати їх для проникнення у вашу мережу. Антивірусне програмне забезпечення виявляє та знищує трояни, шпигунські та інші шкідливі програми на пристрої, перш ніж вони поширяться на решту мережі. Рішення для виявлення та реагування на кінцеві точки – це більш просунуті інструменти, які відстежують поведінку кінцевих точок і автоматично реагують на інциденти безпеки. Уніфіковане програмне забезпечення для керування кінцевими точками допомагає компаніям відстежувати, керувати та захищати всі пристрої кінцевих користувачів з єдиної консолі.

Таким чином, **кібербезпека** – це галузь, що зосереджується на захисті комп'ютерних систем, мереж, програмного забезпечення та даних від кіберзагроз. Вона включає сукупність технологій, процесів та практик, спрямованих на запобігання несанкціонованому доступу, використанню, розголошенню, порушенню цілісності або знищенню інформації.

Таблиця 9.16 – Основні аспекти кібербезпеки

Аспект	Зміст і характеристика
Мережеві брандмауери (firewalls)	Контролюють і фільтрують вхідний і вихідний мережевий трафік на основі встановлених правил безпеки.
Системи виявлення та запобігання вторгненням (IDS/IPS)	Виявляють і запобігають спробам несанкціонованого доступу до мережі.
Антивірусні та антишпигунські програми	Захищають пристрої користувачів від шкідливого програмного забезпечення.
Шифрування даних	Забезпечує конфіденційність даних на пристроях, навіть у випадку їх втрати або викрадення.
Оновлення та патчі	Регулярне оновлення програмного забезпечення для виправлення вразливостей.
Безпечне програмування	Дотримання найкращих практик для уникнення вразливостей у коді.
Багатофакторна аутентифікація (MFA)	Вимагає використання кількох способів підтвердження особи для доступу до системи.
Управління паролями	Використання складних паролів і регулярна їх зміна.
Резервне копіювання	Створення копій важливих даних для захисту від їх втрати.
Політики зберігання та передачі даних	Визначають, як і де повинні зберігатися та передаватися дані для забезпечення їх безпеки.
Системи моніторингу	Постійний нагляд за мережами та системами для виявлення аномальної активності.
План реагування на інциденти	Визначення дій на випадок виявлення кіберзагрози, включаючи усунення наслідків атаки.
Навчання співробітників	Забезпечення навчання щодо кібербезпеки для запобігання соціальній інженерії та іншим методам атак.
Оновлення політик безпеки	Регулярний перегляд і оновлення політик кібербезпеки відповідно до нових загроз.

У сучасному цифровому світі кібербезпека є критично важливою для захисту особистої інформації, конфіденційних даних, фінансових транзакцій, а також для забезпечення безперебійної роботи бізнесу і державних установ. Зловмисні атаки можуть призвести до серйозних наслідків, включаючи фінансові втрати, репутаційні ризики, втрату даних, порушення роботи систем, і навіть загрози національній безпеці. Впровадження ефективних стратегій кібербезпеки та постійне вдосконалення заходів захисту є необхідним для мінімізації ризиків і захисту інформаційних активів.

Безпека комп'ютерних мереж переслідує три основні цілі: запобігання несанкціонованому доступу до мережевих ресурсів; виявляти та припиняти поточні кібератаки та порушення безпеки; І забезпечити, щоб авторизовані

користувачі мали безпечний доступ до потрібних їм мережевих ресурсів, коли вони їм потрібні. Зі збільшенням розміру та складності мереж зростає і ризик кібератак. Наприклад, згідно зі звітом IBM, 82 % витоків даних, з якими стикаються організації, порушення безпеки, які приводить до несанкціонованого доступу до конфіденційної або конфіденційної інформації – стосуються даних, що зберігаються в хмарі. Безпека комп'ютерних мереж захищає цілісність мережевої інфраструктури, ресурсів і трафіку, зупиняючи ці атаки і мінімізуючи фінансові та операційні наслідки. Кібербезпека – будь-яка технологія, захід або практика, спрямована на запобігання кібератакам або пом'якшення їх впливу, яка спрямована на захист систем, програм, IT-обладнання, конфіденційних даних, фінансових активів окремих осіб і організацій від комп'ютерних вірусів, складних і дорогих атак програм-вимагачів, що вимагає регулювання кіберпростору. Умови цифровізації та глобалізації створюють нові виклики і загрози для національної безпеки країн, які варто розглядати в цьому контексті.

Таблиця 9.17 – Нові виклики та загрози у контексті регулювання кіберпростору та забезпечення національної безпеки

Виклики та загрози	Зміст та характеристика
Кібербезпека	Зростання кількості кібератак та злочинної діяльності відкриває широкі можливості для ворогів дізнатися та використовувати конфіденційну інформацію, здійснювати атаки на критичну інфраструктуру та збурювати економічну стабільність.
Інформаційна війна	Глобальні медіа та соціальні мережі створюють нові можливості для маніпуляції громадською думкою, дезінформації та впливу на внутрішні справи інших країн.
Захист критичної інфраструктури	Зростання залежності від цифрових систем управління і критичних інфраструктур, таких як електроенергетика, транспорт і медицина, ставить під загрозу національну безпеку в разі кібератак або технічних збоїв.
Захист персональних даних	Збільшення обсягів збирання та обробки персональної інформації ставить під загрозу приватність громадян і може мати серйозні наслідки для національної безпеки.
Регулювання кіберпростору	Необхідність розробки міжнародних норм і стандартів для контролю за кіберпростором та запобігання конфліктам в мережі.
Кібервійська діяльність	Розвиток нових форм конфлікту, таких як кібервійна діяльність, створює необхідність адаптації стратегій оборони та забезпечення національної безпеки.
Інтернет-свобода та цензура	Боротьба з цензурою в Інтернеті та забезпечення доступу до інформації в умовах глобалізації.
Гібридна війна	Використання різноманітних засобів, включаючи політичний тиск, економічні санкції та дезінформацію, для досягнення політичних цілей та підірвання національної безпеки.

Майбутнє цифрової трансформцаії промислового менеджменту тісно пов'язане із штучним інтелектом. Стандартизована модель управління ризиками великих даних забезпечує відповідність даних користувачів та їх взаємозв'язок у всіх бізнес-сценаріях комерційних операцій, спрощуючи 80 % операційного процесу. Розроблена система захисту від цифрової безпеки спільно сприяє високоякісному розвитку кіберпотужності та цифрового розвитку. Зіткнувшись із ситуацією з мережевою безпекою, що ускладнюється, глобальні технологічні компанії активізують свої дії, так як парадигма цифрової безпеки стійно оновлюється. Microsoft офіційно комерціалізувала Copilot for Security, рішення для автоматизації безпеки, яке може взаємодіяти з природною мовою; Google також випустила минулого року велику модель мережевої безпеки. Компанії, що займаються глобальною безпекою мережі, Palo Alto і Crowd Strike, інтегрували можливості великих моделей у свої платформи забезпечення безпеки. Завдяки хвилі технологій штучного інтелекту Palo Alto стала першою у світі охоронною компанією, ринкова вартість якої перевищує 100 мільярдів доларів США, а ринкова вартість Crowd Strike також наближається до 100 мільярдів доларів США. У Китаї понад 80 % компаній, що займаються мережевою безпекою, інтегрують технології великих моделей у продукти мережевої безпеки, і майже 30 % компаній розпочали дослідження в галузі безпеки великих моделей.

Таблиця 9.18 – Комплексний підхід до співпраці між різними секторами суспільства для забезпечення національної безпеки

Напрямок	Зміст та характеристика
1	2
Кібербезпека	Захист кіберпростору від кібератак, кібершпигунства та кіберсаботажу, розвиток кіберстратегій та кібервійських здібностей для запобігання кіберзагрозам.
Тероризм і радикалізація	Боротьба з тероризмом, радикалізацією та екстремізмом через розвиток превентивних стратегій, співпрацю між розвідувальними службами та залучення громадянського суспільства
Гібридна війна	Використання різноманітних засобів, таких як дезінформація, гібридні атаки, економічний тиск та політичне впливування для досягнення політичних цілей та підірвання стабільності.
Конфлікти і міжнародні кризи	Управління конфліктами, миротворча діяльність та гуманітарна допомога в країнах, що перебувають у конфлікті або під загрозою.
Політична і економічна стабільність	Зміцнення демократії, правової держави та економічної стабільності для запобігання внутрішнім конфліктам та забезпечення національної безпеки.
Збройні сили і оборона	Розвиток та модернізація збройних сил, а також військова доктрина для забезпечення обороноздатності та здатності до реагування на загрози.

Закінчення таблиці 9.18

1	2
Протидія проти поширення зброї масового знищення	Міжнародні зусилля для зменшення ризику поширення ядерної, хімічної та біологічної зброї, контроль за їхнім розповсюдженням та запобігання їхньому використанню.
Міграція та біженці	Управління міграційними потоками, захист біженців та внутрішня безпека в контексті міграційних криз та міжнародної міграції.
Кліматична безпека	Зміна клімату як потенційна загроза для національної безпеки через вплив на ресурси, міграцію та міжнародні конфлікти.
Енергетична безпека	Забезпечення незалежності та стабільності в енергетичному секторі для запобігання політичному тиску та енергетичним кризам.

Вирішення цих проблем вимагає комплексного підходу та співпраці між різними секторами суспільства та міжнародним співтовариством для забезпечення національної безпеки в умовах сучасних викликів і загроз з боку урядів, міжнародних організацій та громадськості для забезпечення стійкості та безпеки в умовах цифрової епохи. Індустрія цифрової безпеки продовжує вдосконалюватися. Дані стають основним стратегічним ресурсом та новим виробничим фактором. Безпека даних стає основною рушійною силою розвитку індустрії цифрової безпеки. У період цифрового інтелекту дані показали три основні зміни.

По-перше, дані стають більш «живими» та створюють великі ризики у складних потоках; схильність до атак стає все більш розширеною, дані змінюються від «дешевих» до «дорогих», їх вартість стає дедалі вищою.

Щоб подолати проблеми безпеки в епоху цифрового інтелекту, необхідно перейти від зосередження уваги на IT до зосередження уваги на бізнесі, від зосередження уваги на обладнанні до зосередження уваги на «людях», від зосередження уваги на будівництві до зосередження уваги на експлуатації.

Необхідно упровадити концепцію мережевої безпеки, посилити захист мережевої безпеки інформаційної інфраструктури, зміцнити побудову механізмів, засобів і платформ координації інформації про мережеву безпеку, посилити вивчення нарощування потенціалу надзвичайних ситуацій для інцидентів мережевої безпеки, активно розвивати індустрію мережевої безпеки, щоб проблеми були попереджені до того, як вони виникнуть. Відповідальність за захист критичної інформаційної інфраструктури має бути реалізована, при цьому галузі та підприємства беруть на себе відповідальність за захист критичної інформаційної інфраструктури як головну мету свого виживання, а компетентні відомства виконують свої регуляторні обов'язки.

Необхідно відповідно до закону жорстко боротися з незаконними та злочинними діями, такими як злом мереж, шахрайство з телекомунікаційними мережами та посягання на приватне життя громадян, долати ланцюжок інтересів у кіберзлочинності, продовжувати формувати ситуацію високого тиску, захищати законні права та інтереси людей. Необхідно проводити глибоку рекламу і популяризацію знань і навичок мережевої безпеки, а також підвищувати обізнаність і навички захисту мережевої безпеки всіх працівників підприємств та організацій.

Необхідно дотримуватися комплексного розвитку освіти, технологій та промисловості з мережевої безпеки, формувати сприятливу екологію підготовки кадрів, технологічних інновацій та промислового розвитку. Необхідно дотримуватися єдності сприяння розвитку та управління відповідно до закону, енергійно культивувати нові технології та нові програми, такі як штучний інтелект, Інтернет речей та мережі зв'язку наступного покоління, активно використовувати закони, правила та стандарти застосування нових технологій.

Необхідно підтримувати цифрову (мережеву, інформаційну, безпеку даних, безпеку додатків), а також посилювати почуття безпеки людей у кіберпросторі. Зусилля з цифрової безпеки повинні бути спрямовані на мережеву безпеку безпеку людей, щоб забезпечувати безпеку особистої інформації та захищати законні права та інтереси громадян у кіберпросторі.

Цифрова безпека більше не є суто технічною проблемою, а є системною інженерією, що охоплює безліч областей, включаючи економістів, філософів,спеціалістів програмного забезпечення, психологів.

Таким чином, здійснюючи цифрову трансформацію промислового менеджменту, керівники підприємств та організацій повинні сформувати сучасну концепцію цифрової безпеки, щоб прискорити побудову системи гарантування безпеки критичної інформаційної інфраструктури, сприймати ситуацію з мережевою безпекою комплексно, посилити можливості захисту мережевої безпеки.

9.3 ЕКОЛОГІЧНА БЕЗПЕКА

Екологічна безпека має вирішальне значення для сталого розвитку людського суспільства на 21 столітті. Екологічна безпека означає стан, при якому екологічне середовище, від якого залежить виживання та розвиток країни, вільне або менш схильне до збитків і загроз, а також має здатність реагувати на основні внутрішні та зовнішні екологічні проблеми для забезпечення постійного стану, включаючи водні джерела, земля, атмосфера. **У вузькому значенні** поняття екологічної безпеки відноситься

до безпеки природних та напівприродних екосистем, тобто до загального рівня відображення цілісності та здоров'я екосистем. Здорова система стабільна та стійка, здатна зберігати свою організаційну структуру та автономію з плином часу залишатися стійкою до стресів. Під екологічною безпекою можна розуміти ступінь захищеності виробництва, життя та здоров'я людини від екологічної шкоди та забруднення навколишнього середовища, включаючи безпеку питної води та харчових продуктів, якість повітря та зеленого середовища тощо. Екологічну безпеку можна визначити як стан та потенціал довкілля та екосистемних послуг, які можуть підтримувати економічний розвиток, соціальну стабільність, забезпечувати засоби для існування та здоров'я людей від забруднення навколишнього середовища та деградації екосистем.

Екологічна безпека ще немає точного визначення. Зазвичай вважається, що воно має два основні значення: перше – не допустити, щоб деградація екологічного середовища становила загрозу для економічної основи, що в основному відноситься до поганої якості довкілля, а також до скорочення та деградації природних ресурсів, які послаблюють здатність підтримувати стійке економічне розвиток. інший – запобігти збиткам навколишнього середовища та природних ресурсів. Нестача ресурсів викликала невдоволення серед людей, особливо велика кількість екологічних біженців, що призвело до заворушень у країні. Екологічна безпека є важливим компонентом національної безпеки та екологічної безпеки, основа та система підтримки регіональної та національної економічної та соціальної стійкості. Екологічна безпека сьогодні в усіх країнах стикається з величезними проблемами, пов'язаними із серйозним забрудненням довкілля, деградацією екосистем та зниженням якості екосистемних послуг. Для підвищення екологічної безпеки необхідно побудувати екологічну систему. моделі безпеки, контролювати забруднення, захищати та відновлювати екосистеми, покращувати екосистемні послуги та підвищувати здатність еко-середовища підтримувати економіку та суспільство.

У широкому значенні це сенс збереження навколишнього середовища та екологічного захисту. Це робиться для того, щоб деградація екологічного середовища не становила загрози для екологічної основи економічного розвитку, що в основному відноситься до поганої якості довкілля, а також до скорочення та деградації природних ресурсів, що послаблюють потенціал екологічної підтримки сталого економічного розвитку. Це робиться для того, щоб економічний спад, спричинений екологічними збитками та нестачею природних ресурсів, не вплинув на умови життя людей, особливо на велику кількість екологічних біженців, що призведе до національних заворушень. Широка концепція екологічної безпеки представлена

визначенням, запропонованим Міжнародним інститутом прикладного системного аналізу (IIASA, 1989): екологічна безпека відноситься до життя, здоров'я, благополуччя людини, основних прав, джерел безпеки життя, необхідних ресурсів. включаючи природну екологічну безпеку, економічну екологічну безпеку та соціальну екологічну безпеку, утворюючи складну штучну систему екологічної безпеки.

Екологічна безпека – це комплекс заходів та стратегій, спрямованих на захист навколишнього середовища від шкідливого впливу людської діяльності, а також на збереження природних ресурсів і забезпечення здорових умов для життя людей. Цей концепт включає різні аспекти, такі як управління відходами, контроль за забрудненням повітря та води, захист біорізноманіття, боротьбу зі змінами клімату та забезпечення стійкості екосистем. Важливість екологічної безпеки полягає в необхідності збереження природних ресурсів для майбутніх поколінь і забезпечення збалансованого розвитку. В умовах зростання промислового виробництва, урбанізації та збільшення чисельності населення, питання екологічної безпеки стає дедалі актуальнішим. Ефективне управління екологічною безпекою вимагає інтеграції екологічних аспектів у всі сфери політики, економіки та соціального життя, а також активної участі громадськості у прийнятті рішень, що впливають на довкілля.

Концепцію екологічної безпеки було запропоновано ще у 1970-х роках. Однак через багатство та складність конотацій екологічної безпеки та відсутності глибоких досліджень екологічної безпеки єдине та загальноприйняте визначення не сформувалося. Визначення екологічної безпеки, як і раніше, має два обмеження: з одного боку, воно враховує лише екологічні ризики (маючи на увазі ймовірність і наслідки несподіваних подій, що відбуваються в конкретній екосистемі), ігноруючи при цьому вразливість (маючи на увазі певні соціальні, політичні, економічні; з іншого боку, екологічна безпека розглядається лише як стан без урахування динамічного характеру екологічної безпеки. У відповідь на це обмеження екологічну безпеку можна визначити як стан існування та його гарантійні умови, за яких людина та природа загалом захищені від несприятливих факторів, завдяки чому вразливість системи постійно підвищується. З одного боку, екологічна безпека означає, що під впливом зовнішніх несприятливих факторів людині та природі не завдається шкоди, не порушуються і не загрожують, може бути забезпечене виживання та розвиток людського суспільства, а природна екосистема може залишатися здоровою та недоторканою. З іншого боку, реалізація екологічної безпеки є динамічним процесом, який потребує постійного поліпшення вразливості для досягнення об'єктивних гарантійних умов для здоров'я та динамічності людини та природи.

Концепція екологічної безпек складається з кількох ключових компонентів, які разом забезпечують комплексний підхід до захисту навколишнього середовища та здоров'я людей.

Таблиця 9.19 – Ключові компоненти концепції екологічної безпеки

Ключовий компонент	**Напрямок розвитку екологічної безпеки**
1	2
Закони та нормативні акти	Встановлення екологічних стандартів та норм, які регулюють викиди забруднюючих речовин, використання природних ресурсів, охорону природних об'єктів тощо.
Міжнародні угоди та співпраця	Участь у міжнародних екологічних угодах, таких як Паризька угода щодо клімату, Конвенція про біорізноманіття, і співпраця з іншими країнами для вирішення глобальних екологічних проблем.
Моніторинг довкілля	Систематичне спостереження за станом довкілля, включаючи моніторинг повітря, води, ґрунтів, і біорізноманіття для виявлення забруднення та інших загроз.
Оцінка впливу на довкілля (ОВД)	Процедура оцінки потенційного впливу на навколишнє середовище різних проектів, включаючи промислові та інфраструктурні проекти, перед їх реалізацією.
Зменшення відходів	Стратегії щодо мінімізації виробництва відходів на всіх етапах виробничих та споживчих процесів.
Переробка та утилізація	Системи збору, переробки та безпечної утилізації відходів для зменшення їх негативного впливу на довкілля.
Очищення води	Забезпечення очищення стічних вод та підтримка якості води в річках, озерах, підземних водах і океанах.
Управління водними ресурсами	Планування і контроль використання водних ресурсів для забезпечення їх стійкого використання.
Контроль викидів	Впровадження технологій та політик для зменшення викидів забруднюючих речовин у повітря, таких як парникові гази, пил, та токсичні хімічні сполуки.
Поліпшення якості повітря	Програми щодо зниження рівня забруднення повітря, включаючи просування використання чистих джерел енергії та транспорту.
Охорона природних територій	Створення і підтримка заповідників, національних парків, та інших охоронюваних територій для збереження видів і екосистем.
Захист видів	Заходи щодо збереження рідкісних та зникаючих видів, а також відновлення популяцій у природному середовищі.
Зменшення енергоспоживання	Впровадження технологій і практик, які підвищують енергоефективність у промисловості, будівництві та побуті.
Розвиток відновлюваної енергетики	Перехід на використання відновлюваних джерел енергії, таких як сонячна, вітрова, гідроенергія, та біомаса, для зменшення залежності від викопних видів палива.

Закінчення таблиці 9.19

1	2
Збереження ґрунтів	Заходи з попередження деградації та ерозії ґрунтів, збереження їх родючості.
Стійке землекористування	Планування використання земель з урахуванням екологічних аспектів для збереження природних екосистем.
Екологічна освіта	Інформування та навчання населення щодо важливості екологічної безпеки та впровадження екологічно дружніх практик.
Просування екологічних цінностей:	Формування в суспільстві розуміння важливості збереження навколишнього середовища через медіа, громадські кампанії та освіту.
Зелений бізнес	Стимулювання розвитку бізнесів, які мінімізують негативний вплив на довкілля, сприяють сталому розвитку та підтримують циркулярну економіку.
Еко-інновації	Інвестування у нові технології та процеси, що зменшують вплив на довкілля, підвищують ефективність використання ресурсів і підтримують стійкість екосистем.

В основі концепції екологічної безпеки врахування природа екологічної безпеки, яка має два аспекти: екологічний ризик та екологічна вразливість. Екологічний ризик є ймовірністю і наслідками шкоди, заподіяної екологічним тиском. Умовно кажучи, він більше враховує шкоду від надзвичайних ситуацій та менше ініціативи та ентузіазму щодо управління шкодою, тоді як екологічну вразливість слід назвати основою екологічної безпеки. За допомогою аналізу та оцінки вразливостей ми можемо дізнатися, які загрози екологічній безпеці, як вони працюють та які стратегії реагування та адаптації люди можуть прийняти. Відповівши на ці питання, ми зможемо активно та ефективно захищати екологічну безпеку. Отже, наукова суть екологічної безпеки полягає у використанні різних засобів для постійного підвищення вразливості та зниження ризиків за допомогою аналізу та оцінки вразливості. Екологічна безпека підкреслює, що до екосистем, що забезпечують екологічну безпеку, повинні належати природні екосистеми, штучні екосистеми та природно-штучні складні екосистеми. За обсягом його можна розділити на кілька рівнів, таких як глобальна екосистема, регіональна екосистема і мікроекосистема.

З екологічної точки зору безпечна екосистема може зберігати свою організаційну структуру протягом певного періоду часу та зберігати стійкість до стресів. Тобто вона може не тільки задовольняти потреби розвитку людини в ресурсах і навколишньому середовищі, а й мати екологічну стійкість. значення. Суть екологічної безпеки полягає в тому, щоб

вимагати стабільного, скоординованого, впорядкованого та сталого використання природних ресурсів за дотримання трьох обмежень: населення, соціальна економіка та екологічне середовище. Зі зростанням чисельності населення та соціально-економічного розвитку тиск діяльності людини на навколишнє середовище продовжує зростати, загострюється протиріччя між людиною та землею. Хоча країни всього світу досягли значних успіхів у побудові екологічного середовища, вони не змогли фундаментально повернути назад тенденцію зворотної еволюції навколишнього середовища, екологічні та екологічні катастрофи, викликані деградацією навколишнього середовища та екологічним руйнуванням, не були пом'якшені, і глобальні зміни не були пом'якшені. Потепління, підвищення рівня моря, виникнення та швидке розширення озонової діри, різке скорочення біорізноманіття – це глобальні екологічні проблеми, пов'язані з безпекою людини, які знову і знову б'ють на сполох перед людством.

Безпека окремих людей, населених пунктів, поселень, регіонів та країн стикається з проблемами з боку екологічного середовища. Екологічна безпека займає таке ж важливе стратегічне становище, як і національна оборонна безпека, економічна безпека та фінансова безпека і становить важливу частину національної безпеки та регіональної безпеки. Підтримка глобальної та регіональної екологічної безпеки, екологічної безпеки та сталого економічного розвитку стала загальним консенсусом міжнародного співтовариства та людства.

Концепція екологічної безпеки має характеристики цілісності, незворотності та довгострокового характеру.

Таблиця 9.20 – Визначення екологічної безпеки

Ключовий компонент	**Визначення екологічної безпеки**
1	2
Стан довкілля людини або екологічних умов існування людини	Екологічна безпека – стан довкілля людини або екологічних умов існування людини, необхідна екологічна умова та екологічний стан, необхідна умова екосистеми для виживання та розвитку людини, у взаєминах між людиною та навколишнім середовищем.
Відносна безпека, яка складається з багатьох чинників, може бути кількісно оцінена	Екологічна безпека – відносна безпека, яка складається з багатьох чинників, їхня задоволеність виживанням і розвитком людства варіюється, як і задоволеність екологічною безпекою. Якщо для подання ступеня задоволеності екологічної безпеки використовується коефіцієнт екологічної безпеки, то рівень забезпечення екологічної безпеки в різних місцях може бути різним. Екологічна безпека може бути кількісно оцінена за допомогою показників оцінена.

Закінчення таблиці 9.20

1	2
Динамічний стан концепції	Екологічна безпека – динамічна концепція, не фіксується раз і назавжди, може змінюватись в залежності від змін навколишнього середовища та зворотного зв'язку з умовами життя, виживання та розвитку людини, призводячи до змін ступеня безпеки або навіть від безпеки до небезпеки.
Людина на першому місці	Екологічна безпека ставить людей перше місце. Рівень безпеки та небезпеки вимірюється якістю екологічних факторів, необхідних людині, щоб задовольнити потреби нормального виживання та розвитку людини.
Просторові та регіональні характеристики	Екологічна безпека має певні просторові та регіональні характеристики, загрози екологічної безпеки часто мають регіональний та локальний характер, екологічні катастрофи призводять до глобальних наслідків для всього людства.
Регулювання екологічної безпеки	Екологічну безпеку можна регулювати, вжити заходів щодо усунення екологічних катастроф та перетворення небезпечних факторів на безпечні, зменшити небезпечні стани та території завдяки упровадженню екрологічної безпеки.
Загрози екологічній безпеці	Підтримка екологічної безпеки потребує витрат, загрози екологічній безпеці часто походять від діяльності людини. Діяльність людини завдає шкоди довкіллю, внаслідок чого її власні екосистеми ставлять під загрозу самі себе. Це слід враховувати при розрахунку вартості людського розвитку та розвитку.
Рамки екологічної безпеки	Рамки екологічної безпеки включають здоров'я, цілісність та стійкість екосистем, екосистемні послуги, а також аналіз та оцінку екологічної безпеки. Концепція екологічної безпеки включає: 1) оцінка здоров'я екосистем та екологічного ризику; 2) національні інтереси в галузі екологічної безпеки; 3) модель підтримки прийняття рішень для регіонального сталого розвитку.

Екологічна безпека як міждисциплінарна галузь природничих та соціальних наук передбачає: 1) здоров'я, цілісність та стійкість екосистем; 2) екосистемні послуги, що сприяють добробуту людини. Національна екологічна безпека має на увазі, що країна має повний набір екосистем, які вільні від загроз та підтримують виживання та розвиток країни, і що країна має можливість вирішувати основні екологічні проблеми. Екологічна безпека включає внутрішні ресурси, водні об'єкти, а також екологічну та біологічну безпеку. Це одночасно і мета сталого розвитку, і динамічна система, схильна до постійного розвитку. Екологічна безпека, як важливий компонент національної безпеки, є передумовою політичної, військової та економічної безпеки та впливає на суспільний добробут, стійкий економічний

та соціальний розвиток та довгострокову стабільність. Вона є однією з основ усієї системи національної безпеки. Поряд із прогресом у побудові екоцивілізації Китай підвищив своє розуміння екологічної безпеки, дотримуватися цілісного підходу до національної безпеки та створення системи національної безпеки, яка інтегрує політичну, внутрішню, військову, економічну, культурну, соціальну, науково-технічну, інформаційну, екологічну, ресурсну та ядерну безпеку. Китай розвивається шляхом сталого розвитку, заснованого на збільшенні виробництва, підвищенні рівня життя і здорових екосистемах, має продовжити концепцію створення добрих умов праці та життя для людей та відігравати роль у забезпеченні глобальної екологічної безпеки, створити систему екологічної безпеки, приділяючи першорядну увагу екосистемам, що добре функціонують, та ефективному контролю екологічних ризиків, які він назвав однією з п'яти систем-компонентів екоцивілізації.

Створення системи екологічної безпеки – це складний, важкий та систематичний проєкт, що потребує тривалих зусиль. Це стратегічний захід щодо покращення системи національної безпеки, маючи на увазі запобігання проблемам екологічної деградації та ефективну підтримку економіко-соціального розвитку та добробуту людини за рахунок екосистемних послуг. Однак протягом тривалого часу розуміння концепції та конотації екологічної безпеки варіювалося серед дослідників та осіб, які приймають рішення, а фокуси та підходи оцінки екологічної безпеки також не були уніфіковані з різноманітними обмеженнями, які, очевидно, не сприяли відповідним дослідженням та практиці.

Проблеми екологічної безпеки стали серйозною проблемою, пов'язаною із благополуччям людей та майбутнього нації, для чогонадавати великого значення як традиційній, так і нетрадиційній безпеці та будувати систему, яка об'єднує політичну безпеку, внутрішню безпеку, військову безпеку, економічну безпеку, культурну безпеку, соціальну безпеку, наукову та технологічну безпеку. Інформаційна безпека, екологічна безпека, ресурсна безпека та ядерна безпека – це інтегрована система національної безпеки. Це велике стратегічне розгортання, засноване на точному розумінні нових характеристик та тенденцій зміни ситуації у сфері національної безпеки. Воно має велике значення для підвищення обізнаності щодо важливості екологічної безпеки та боротьби з загрозами екологічної безпеки. Для цього маємо дотримуватися зеленого розвитку, впорядковано використати природу та побудувати наукову та розумну модель екологічної безпеки.

Екологічна безпека, як і політична безпека, військова безпека та економічна безпека, є областю безпеки, яка стосується загальної ситуації та істотно впливає на національну безпеку. Екологічна безпека є носієм

та основою іншої безпеки і водночас зазнає впливу та обмеження іншої безпеки. Для забезпечення плавної реалізації національної стратегії екологічної безпеки необхідно посилити побудову систем та механізмів, інтегрувати відповідні організаційні структури та уточнити обов'язки кожного відомства. На національному рівні має бути створений ефективний механізм нагляду, оцінки та підзвітності для забезпечення ефективності реалізації національної стратегії екологічної безпеки. Забезпечення національної екологічної безпеки невіддільне від технічної підтримки. Необхідно повною мірою використовувати технології для створення всеосяжної бази даних національної екологічної безпеки та прогнозування майбутньої ситуації національної екологічної безпеки, а також просторового та тимчасового розподілу інформації за допомогою аналізу та оцінки поточного стану та динаміки екологічної безпеки. Національна екологічна безпека сама по собі є великим системним проектом, і розробка на найвищому рівні має бути зосереджена на національному рівні. Необхідно зосередити увагу на ключових питаннях, інтегрувати різні існуючі великі проекти, побудувати механізм координації та зв'язків для захисту довкілля, економічного розвитку та покращення життя людей, максимально підвищити ефективність використання робочої сили, матеріальних ресурсів та засобів, а також максимізувати екологічну безпеку.

Екологічна безпека, як і політична безпека, військова безпека та економічна безпека, є областю безпеки, яка стосується загальної ситуації та істотно впливає на національну безпеку. Екологічна безпека є носієм та основою іншої безпеки і водночас зазнає впливу та обмеження іншої безпеки. Для забезпечення плавної реалізації національної стратегії екологічної безпеки необхідно посилити побудову систем та механізмів, інтегрувати відповідні організаційні структури та уточнити обов'язки шкірного відомства. На національному рівні має бути створений ефективний механізм нагляду, оцінки та підзвітності для забезпечення ефективності реалізації національної стратегії екологічної безпеки. Забезпечення національної екологічної безпеки невіддільне від технічної підтримки. Необхідно повною мірою використовувати технології для створення всеосяжної бази даних національної екологічної безпеки та прогнозування майбутньої ситуації національної екологічної безпеки, а також просторового та временного розподілу інформації за допомогою аналізу та оцінки поточного стану та динаміки екологічної безпеки.

Визначення, запропоноване Міжнародним інститутом прикладного системного аналізу (1989 р.): екологічна безпека відноситься до людського життя, здоров'я, благополуччя, основних прав, джерел безпеки життя, необхідних ресурсів, соціального порядку та адаптації людини

до навколишнього середовища. Держава, в якій здатність до зміни та інші аспекти не перебувають під загрозою, включаючи природну екологічну безпеку, економічну екологічну безпеку та соціальну екологічну безпеку. Екологічна безпека інколи перетинає національні кордони. Екологічна катастрофа в одній країні може загрожувати екологічній безпеці сусідніх країн. Наприклад, у міжнародних річках скидання або витік забруднюючих речовин у країнах верхньої течії може поставити під загрозу водну безпеку країн нижньої течії. Деякі екологічні та екологічні проблеми навіть загрожують глобальній екологічній безпеці.

Екологічна безпека відноситься до цілісності екосистем і біосфери, особливо по відношенню до їх здатності підтримувати різноманітність форм життя (включаючи людське життя). Безпека екосистем привертає все більшу увагу в міру зростання впливу екологічної шкоди з боку людини. [24] Деградація екосистем, включаючи ерозію верхнього шару ґрунту, вирубку лісів, втрату біорізноманіття та зміну клімату, впливають на економічну безпеку та можуть прискорити масову міграцію, що призведе до збільшення тиску на ресурси в інших місцях. Екологічна безпека також важлива, оскільки більшість країн світу розвиваються і залежать від сільського господарства, а сільське господарство страждає багато в чому через зміну клімату. Цей ефект впливає на економіку країни, що в свою чергу позначається на національній безпеці. Масштаб і характер екологічних загроз національній безпеці та стратегії їх подолання є предметом дискусій. Ромм (1993) класифікує основні впливи екологічних змін на національну безпеку як:

Транснаціональні екологічні проблеми. До них належать глобальні екологічні проблеми, такі як зміна клімату через глобальне потепління, вирубку лісів та втрату біорізноманіття.

Місцевий екологічний або ресурсний тиск. До них відносяться нестача ресурсів, що призводить до локальних конфліктів, таких як суперечки щодо нестачі води на Близькому Сході; міграція в США, викликана провалом сільського господарства в Мексиці; вплив на конфлікт в Сирії ерозії продуктивних земель. Відсутність екологічної безпеки в Руанді після зростання населення та зменшення доступності сільськогосподарських угідь, можливо, також сприяла геноциду там.

Екологічно небезпечні наслідки ведення війни. До них належать воєнні дії, які деградують або руйнують екосистеми. Прикладами є руйнування римлянами сільського господарства в Карфагені; спалення Саддамом Хусейном нафтових свердловин під час війни в Перській затоці; використання Agent Orange Великою Британією під час надзвичайної ситуації в Малайї та США під час війни у В'єтнамі для дефоліації лісів. Зміна клімату впливає на світове сільське господарство та продовольчу безпеку.

Національна екологічна безпека сама по собі є великим системним проектом, і розробка на найвищому рівні має бути зосереджена на національному рівні. Необхідно зосередити увагу на ключових питаннях, інтегрувати різні існуючі великі проекти, побудувати механізм координації та зв'язків для захисту довкілля, економічного розвитку та покращення життя людей, максимально підвищити ефективність використання робочої сили, матеріальних ресурсів та засобів, а також максимізувати екологічну безпеку, переваги. Уряди повинні дотримуватися політики пріоритету збереження, захисту та природного відновлення, а також прагнути до створення екологічних концепцій, удосконалення екологічних систем, підтримки екологічної безпеки та оптимізації екологічного середовища. Для цього ми маємо прискорити будівництво систем та механізмів та зробити все можливе для підтримки екологічної безпеки з високим ступенем відповідальності перед людьми.

Для цього слід зміцнити будівництво національної екологічної безпеки та верховенства закону. Побудова верховенства права є важливим символом соціального прогресу та необхідною гарантією досягнення країною екологічної безпеки.

По-перше, в даний час екологічному законодавству не вистачає системності та повноти, і явище множинного та вибіркового правозастосування все ще існує. Для посилення ролі правового захисту національної екологічної безпеки насамперед необхідно посилити законотворчу роботу. На основі різних існуючих законів та постанов, а також виходячи з потреб національної екологічної безпеки, слід вдосконалити національну систему правової підтримки екологічної.

По-друге, посилити правоохоронну діяльність. У разі великих подій, пов'язаних із національною екологічною безпекою, необхідно здійснювати спільну правоохоронну діяльність кількох відомств, щоб сумісно реалізувати концепцію екологічної безпеки.

По-третє, покращення демократичної системи контролю. Необхідно керівникам та співробітникам певних фірм та організацій енергійно оволодівати юридичною освітою в галузі екологічної безпеки, розвивати поінформованість про екологічну безпеку серед кадрів, активно контролювати поведінку, яка ставить під загрозу екологічну безпеку країни, та формувати соціально-правове середовище.

По-четверте, для забезпечення безперебійної реалізації національної стратегії екологічної безпеки необхідно посилити побудову систем та механізмів, інтегрувати відповідні організаційні структури та уточнити обов'язки кожного відомства. На національному рівні має бути створений ефективний механізм нагляду, оцінки та підзвітності для забезпечення ефективності реалізації національної стратегії екологічної безпеки.

По-п’яте, створити національну систему оцінки екологічної безпеки та раннього попередження. Забезпечення національної екологічної безпеки невіддільне від технічного забезпечення.

Необхідно повністю вивчити та використовувати великі дані, комплексно використовувати просторовий аналіз, інтеграцію інформації, Інтернет + та інші технології для створення всеосяжної бази даних національної екологічної безпеки, а також прогнозувати майбутню ситуацію національної екологічної безпеки та просторовий розподіл за допомогою аналізу та оцінки. сучасного стану та динаміки екологічної безпеки. На цій основі має бути створена національна система оцінки екологічної безпеки та раннього попередження, а також має бути створена платформа оцінки попередження, випуску та реагування для повного захисту екологічної безпеки моєї країни.

Створення великих національних про’ктів з екологічної безпеки. За останні роки наша країна здійснила низку великих природоохоронних та будівельних проектів і досягла чудових результатів. Однак проектування деяких проектів на верхньому рівні не вистачає системності та цілісності, основна увага приділяється «управлінню на кінці труби» і є екстрена функція «лікування голови, коли болить, і ноги, коли болить». Національна екологічна безпека сама по собі є великим системним проектом, і розробка на найвищому рівні має бути зосереджена на національному рівні. Необхідно зосередити увагу на ключових питаннях, інтегрувати різні існуючі великі проекти, побудувати механізм координації та зв’язків для захисту довкілля, економічного розвитку та покращення добробуту населення, максимізувати ефективність використання робочої сили, матеріальних ресурсів та коштів, а також максимізувати екологічну безпеку, переваги. Тиск на систему Землі продовжує зростати в міру загострення таких проблем, як втрата біорізноманіття, зміна клімату та забруднення довкілля. Сім основних проблем, пов’язаних із земною системою, створили серйозні проблеми для національної безпеки.

Керівникам підприємств та організацій необхідно адаптувати систему безпеки, щоб краще реагувати на мінливу картину ризиків, домогтися співпраці за участю багатьох зацікавлених сторін. У міру наближення до середини XXI століття ситуація в галузі глобальної безпеки стає все більш складною та серйозною. Російсько-українська війна, Близький Схід та країни Африки на південь від Сахари, не лише перешкоджають міжнародним миротворчим зусиллям, але й посилюють гуманітарні кризи та викликають громадянські протести. Азія, Латинська Америка та інші частини Африки також стикаються з цілою низкою проблем безпеки, таких як політична нестабільність, організована злочинність та корупція.

Геополітичні потрясіння привернули увагу всього світу, і в той же час посилюється множинний тиск на систему Землі, таку як втрата біорізноманіття, зміна клімату та забруднення. Крім того, ми також можемо стати свідками незворотних збитків, завданих перевищенням екологічних переломних моментів на коралових рифах та льодовиковому щиті Гренландії. Цей тиск вплине на глобальну безпеку людства.

Існуюча модель безпеки ґрунтується на минулій Землі, якої більше не існує. Без втручання сьогоднішня геополітична нестабільність та стрес системи Землі, ймовірно, спровокують безпрецедентну та неконтрольовану глобальну кризу безпеки. Тому існує гостра необхідність включення вищезгаданих факторів у відповідні структури безпеки. Діяльність людини сильно змінила образ Землі. Обговорення проблем безпеки часто зосереджуються навколо зміни клімату та тиску, який він чинить на системи Землі, але ігнорують критичний тиск на живі істоти та наслідки забруднення. Деградація ґрунту, виснаження прісної води, перевантаження поживними речовинами та інші планетарні стреси в сукупності створюють складні екологічні проблеми, що стосуються безпеки. Норми безпеки, які віддають пріоритет зміні клімату, ігноруючи при цьому інші джерела стресу, є неповними і можуть навіть становити загрозу. Кожен тиск матиме унікальний вплив на глобальну екологічну ситуацію та ситуацію з безпекою, наголошуючи на необхідності комплексного підходу до зміни норм безпеки.

Грунтуючись на визначенні та аналізі екологічної безпеки, проведеному різними вченими, з точки зору вимог до підтримки екологічного середовища для сталого розвитку економіки та суспільства, екологічна безпека може бути у такій мірі, коли екологічні умови довкілля та функції екосистемних послуг можуть ефективно підтримувати економічний розвиток та соціальну стабільність, щоб захистити життя та здоров'я людей від забруднення навколишнього середовища та екологічної шкоди. Екологічна безпека є основою екологічного середовища та опорою регіональної та національної економічної та соціальної безпеки. Концепція екологічної безпеки має такі п'ять характеристик:

По-перше, ядро екологічної безпеки орієнтоване людей. Екологічна безпека вимагає захисту здоров'я екологічного середовища, щоб продовжувати надавати екологічні продукти та послуги, забезпечувати систему життєзабезпечення для виживання людини, забезпечувати екологічну підтримку економічного розвитку та запобігати загрозі соціальної стабільності екологічними та екологічними проблемами. полягає в тому, щоб поєднати людей і Природу як референт безпеки, що, по суті, є безпекою людини, безпекою людського виживання та розвитку. Стандарти безпеки

вимірюються якістю та кількістю екосистемних продуктів та послуг, необхідних для виживання та розвитку людини.

По-друге, хороше екологічне середовище є матеріальною основою екологічної безпеки. Умови та матеріальні ресурси, які екосистеми забезпечують для виживання, виробництва та життя людини, включаючи екосистемні продукти та послуги. Екосистемні продукти включають продукти харчування, деревину, волокно, ресурси прісної води, генетичний матеріал, що надаються екосистемою, і можуть бути використані безпосередньо людьми. Екосистемні послуги включають формування та підтримання умов для виживання та розвитку людини, таких як виробництво органічних речовин, переробка поживних речовин, регулювання клімату, регулювання гідрології, збереження ґрунтів, регулювання повеней, деградація забруднюючих речовин, секвестрація вуглецю, виробництво кисню та інше екологічне регулювання. функції, а також екологічні та культурні функції, такі як літературне та художнє натхнення, знання, освіта та естетика ландшафту, отримані з компонентів та процесів екосистеми. Люди поступово усвідомлюють, що продукти та послуги, які надаються екосистемами, є основою виживання людства та сучасної цивілізації. Суть регіональних та глобальних екологічних та екологічних проблем полягає у пошкодженні та ослабленні сервісних функцій екосистем. Тому ефективний контроль забруднення навколишнього середовища, захист та відновлення природних екосистем, покращення функцій екосистемних послуг та покращення здатності екологічного середовища підтримувати економіку та суспільство є основними заходами щодо забезпечення екологічної безпеки.

По-третє, екологічна безпека – це підтримка сталого економічного та розвитку. Забезпечення екологічної безпеки означає забезпечення екосистемних продуктів та послуг, на які люди покладаються для виживання та розвитку, таких як безперервне постачання продовольства, чистого повітря та води, а також запобігання та пом'якшення впливу стихійних лих на економіку та суспільство за допомогою таких функцій, як: збереження ґрунту, захист від вітру та фіксація піску, а також регулювання гідрологічної шкоди. Норман Майєрс підкреслив у своїй книзі «Абсолютна безпека: екологічна основа політичної стабільності», що гарантія національної безпеки більше не включає лише військову міць і зброю, але все частіше включає водні потоки, оброблювані землі, ліси та генетичні ресурси, клімат і ресурси. інші чинники довкілля. Поки екологічне середовище продовжує завдавати збитків, остаточної політичної та економічної безпеки не буде. Оскільки деградація довкілля погіршує місце існування, це призведе до занепаду економічної основи країни, а її політична структура також стане нестабільною, що може викликати соціальні заворушення або

напруженість і конфлікти з іншими країнами [10]. Деградація екосистем та втрата функцій екологічних послуг можуть навіть поставити під загрозу умови життя всієї країни та нації.

По-четверте, екологічна безпека має регіональний взаємний вплив та залежність. Через відмінності в кліматі, географії, структурах та процесах екосистем екологічні та екологічні проблеми, очевидно, мають регіональний характер. Наприклад, кам'янисте опустелювання в основному відбувається в районах поширення карсту, тоді як опустелювання в основному відбувається в посушливих та напівзасушливих районах, викликаючи деградацію екосистем. Геологічні катастрофи посилюються переважно в гірських районах південного заходу з високими горами, крутими схилами і концентрацією опадів. Різні регіони можуть стикатися з різними проблемами екологічної безпеки. Регіональне співвідношення екологічної безпеки зазвичай відображається у двох аспектах: взаємний вплив та взаємозалежність. З одного боку, багато проблем екологічної безпеки пов'язані з регіоном. Деградація екологічних функцій в одному регіоні загрожує екологічній безпеці іншого регіону.

По-п'яте, екологічна безпека відносна та динамічна. Проблеми екологічної безпеки динамічно змінюються. З часу промислової революції здатність людей втручатися в природне середовище продовжувала покращуватися, а екологічні та екологічні проблеми, з якими стикаються люди, також змінювалися залежно від періодів та стадій розвитку. Від руйнування довкілля людини, такого як забруднення водного середовища, повітря і ґрунту, до погіршення довкілля людини, такого як парниковий ефект, глобальна зміна клімату, втрата біорізноманіття, руйнування озонового шару та деградація екологічних послуг. Функції, екологічні проблеми, з якими стикається людство, мають проблеми безпеки, постійно змінюються і розвиваються, а екологічний тиск, з яким стикається людство, стає все більш серйозним. В екологічній безпеці немає абсолютної безпеки, є лише відносна безпека. З розвитком економіки та суспільства, великомасштабним освоєнням ресурсів, змінами у землекористуванні, викидами забруднювачів навколишнього середовища, надмірним використанням лісів, лук, водно-болотних угідь та біологічних ресурсів, а також розвитком та застосуванням науки та техніки, деякі екологічні та екологічні проблеми вирішені, та знову виникнуть нові екологічні та екологічні проблеми. Здається, що кожного разу, коли людська цивілізація розвивається, виникають нові екологічні та екологічні проблеми, і кожен прогрес, здається, досягається за рахунок екологічної безпеки.

Екологічні проблеми, такі як парниковий ефект, зміна клімату, втрата біорізноманіття та виснаження озонового шару можуть завдати шкоди добробуту

та здоров'ю всього людства. Захист навколишнього середовища є важливою частиною національної та міжнародної безпеки, а екологічна деградація є серйозною загрозою, так як є явні ознаки того, що нестача екологічних ресурсів може сприяти насильницьким конфліктам у багатьох частинах світу. У найближчі десятиліття зростання тиску на довкілля може змінити основу глобальної політичної ситуації. Деградація земель, в основному ерозія ґрунту, опустелювання земель та кам'янисте опустелювання, як і раніше, залишається серйозною проблемою. Втрата ґрунту та води широко поширена та охоплює велику територію по всій країні. Опустелені землі займають велику площу і переважають украй важкі та сильні ступеня опустелювання. Тенденція штучності екосистем ще більше посилилася, а природні житла диких тварин і рослин скоротилися. Екологічна ситуація в річкових басейнах Китаю є важкою: річки висихають, зникають водно-болотні угіддя, водне середовище серйозно забруднене, біорізноманіття скорочено, а функції екологічного регулювання перебувають на низькому рівні. Забудовані території більшості ключових міст наслідують моделі одноцентрового розширення, подібно до розкладання пирога. Розширення міст виходить з-під контролю, функція екологічного регулювання постійно знижується, середовище населених пунктів погіршується. «Ефект острова тепла» у всіх великих містах країни продовжує посилюватися, часто відбуваються заболочування, міські зелені насадження мають просту структуру, висока частка екзотичних рослин та дедалі більша кількість рослин, що викликають алергію на пилок, мають серйозний вплив. про життя городян.

Екологічні катастрофи відбуваються часто і завдають великої шкоди життю та майну людей. Через погіршення стану довкілля різні стихійні лиха стали більш серйозними та руйнівними, що стало ще однією величезною проблемою, з якою стикається екологічний захист. До основних із них відносяться часті піщані бурі, серйозна небезпека селів, широке осідання земель, а також посилення повеней та посух. Геологічні катастрофи безпосередньо чи опосередковано тісно пов'язані з деградацією місцевих екосистем. Екологічні проблеми, спричинені освоєнням ресурсів, продовжують загострюватись. Швидке економічне зростання та швидка урбанізація сприяли широкомасштабному освоєнню ресурсів, формуючи безпрецедентну інтенсивність та масштаб освоєння ресурсів. Зокрема, освоєння водних ресурсів, розвиток гідроенергетики, освоєння викопних джерел енергії, освоєння мінеральних ресурсів тощо надали негативний вплив. на екологічне середовище та створило низку нових екологічних та екологічних проблем.

Водні ресурси душу населення низькі, а просторове розподіл водних ресурсів нерівномірно. Екологічні проблеми, спричинені надмірною експлуатацією водних ресурсів, швидко поширилися, що призвело до дисбалансу

в балансі водної екосистеми, постійного зниження рівня ґрунтових вод, втрат озер та водно-болотних угідь, висихання річок та осідання земель. Подібні екологічні проблеми швидко поширилися і стали величезною загрозою сталому економічному та соціальному розвитку щодо розвинених регіонів. Надмірна експлуатація підземних вод призвела до падіння рівня ґрунтових вод та появи великомасштабних вирв підземних вод. Розробка мінеральних ресурсів завдала серйозних збитків екологічному середовищу та викликала серйозне забруднення навколишнього середовища.

Щоб підтримати стійкий розвиток економіки та суспільства, основна ідея стратегії екологічної безпеки має полягати в тому, щоб побудувати екологічну цивілізацію як мету, впровадити вимоги захисту екологічного середовища до економічного будівництва та соціального розвитку, а також побудувати модель національної екологічної безпеки та контроль забруднення навколишнього середовища. середовища, захист природних екосистем, усунення екологічних та екологічних проблем, розгортання регіональних екологічних будівельних проектів та створення довгострокових механізмів екологічного та екологічного захисту для підвищення здатності екологічного середовища підтримувати економіку. розвиток та соціальна стабільність. Таким чином, екологічна безпека включає захист навколишнього середовища, націлений на організацію постійного спостереження за станом довкілля для виявлення та попередження екологічних загроз, таких як забруднення повітря, води, ґрунтів, радіоактивне зараження, деградація екосистем, організацію та проведення робіт з ліквідації наслідків екологічних катастроф, таких як розливи нафти, викиди хімічних речовин, лісові пожежі, зсуви, а також відновлення природних ресурсів (табл. 9.21).

Теоретичне і практичне значення впровадження екологічної безпеки є важливим аспектом сучасного розвитку суспільства, який має глибокі наслідки для навколишнього середовища, економіки, здоров'я людей та соціальної стабільності. Це питання стає все більш актуальним в умовах глобальних екологічних викликів, таких як зміна клімату, забруднення довкілля, зниження біорізноманіття та виснаження природних ресурсів. Впровадження екологічної безпеки сприяє розробці та впровадженню концепцій сталого розвитку, що поєднують економічний розвиток, соціальний прогрес і захист довкілля. Теоретичні основи екологічної безпеки допомагають визначити оптимальні шляхи досягнення гармонії між економічною діяльністю і збереженням природних екосистем. Вивчення теоретичних аспектів екологічної безпеки сприяє розвитку екологічної етики, яка включає моральні принципи щодо взаємодії людини з природою. Це дозволяє формувати у суспільстві відповідальне ставлення до природних ресурсів і навколишнього середовища.

Таблиця 9.21 – Практичні рекомендації удосконалення екологічної безпеки

Ключовий компонент	Напрямок удосконалення
1	2
Створити національну модель екологічної безпеки та забезпечити безперервне надання екосистемних послуг	Створити національну модель екологічної безпеки та забезпечити безперервне надання екосистемних послуг. Дотримуватись реалізації планування основної функціональної зони, координувати взаємозв'язок між розвитком та захистом екологічного середовища, сприяти коригуванню промислового планування та здійснення екологічних та природоохоронних заходів. Модель екологічної безпеки включає потреби екологічної безпеки з плануванням зон обмеженого розвитку національних та місцевих функціональних зон, що зосереджуються на важливих екологічних функціях, таких як збереження джерел води, захист від вітру та фіксація піску, регулювання та зберігання повеней, захист біорізноманіття, збереження води та ґрунту.
Поліпшити національну систему класифікації землекористування	Поліпшити національну систему класифікації землекористування, збільшити кількість типів екологічних земель, основною метою яких є забезпечення функцій екосистемних послуг, впровадити екологічні землі у загальне планування землекористування на всіх рівнях та запланувати території з надзвичайно важливими функціями екологічних послуг. Будівництво мережі екологічного захисту має бути посилено, щоб сформувати національну систему екологічного захисту з природними заповідниками, національними парками та заповідниками з важливими екологічними функціями, щоб закласти основу для побудови національної моделі екологічної безпеки.
Посилити захист навколишнього середовища	Посилити захист навколишнього середовища, включаючи контроль за викидамив забруднюючих речовин та покращення міської та сільської зони навколишнього середовища, збереження водних джерел, збереження ґрунту та води, захист від вітру та фіксація піску, підтримання біорізноманіття, запобігти та стримати утворення «зелених пустель». Екологічне будівництво постало перед «дилемою» збільшення рослинного покриву та зниження екологічних функцій.
Продовжувати просувати регіональні екологічні будівельні проєкти	Продовжувати просувати регіональні екологічні будівельні проєкти, зосередитися на важливих екологічних функціональних областях з важливим збереженням водних джерел, захистом від вітру та фіксацією піску, регулюванням повеней, захистом біорізноманіття, збереженням води та ґрунту та іншими функціями для розробки великих регіональних екологічних будівельних проєктів.
Забезпечити екологічну безпеку об'єктів капітального будівництва	Забезпечити екологічну безпеку об'єктів капітального будівництва. Посилити роботу з екологічного захисту та екологічного відновлення у галузі розробки мінеральних ресурсів, проєктів розвитку гідроенергетики річкових басейнів та великих проєктів будівництва інфраструктури. Насамперед необхідно посилити оцінку впливу на довкілля розробки мінеральних ресурсів, проектів розвитку гідроенергетики річкових басейнів.

Закінчення таблиці 9.21

1	2
Забезпечити екологічну безпеку об'єктів капітального будівництва	Забезпечити екологічну безпеку об'єктів капітального будівництва. Посилити роботу з екологічного захисту та екологічного відновлення у галузі розробки мінеральних ресурсів, проектів розвитку гідроенергетики річкових басейнів та великих проектів будівництва інфраструктури. Насамперед необхідно посилити оцінку впливу на довкілля розробки мінеральних ресурсів, проектів розвитку гідроенергетики річкових басейнів та планування проектів будівництва великих об'єктів інфраструктури.
Створити довгостроковий механізм координації розвитку та захисту навколишнього середовища	Створити довгостроковий механізм координації розвитку та захисту навколишнього середовища. У зв'язку з урбанізацією необхідно енергійно розвивати освіту в ключових галузях екологічного захисту та екологічного будівництва для підвищення рівня екологічної освіти.

Теоретичні дослідження в галузі екологічної безпеки сприяють розробці законодавчих актів і нормативних документів, які регулюють діяльність людини з метою захисту довкілля. Вони також допомагають визначити юридичні механізми відповідальності за екологічні правопорушення. Теоретичні основи екологічної безпеки дозволяють створювати моделі прогнозування екологічних ризиків і наслідків антропогенної діяльності. Це сприяє підвищенню точності оцінки потенційних загроз для довкілля та розробці превентивних заходів.

9.4 ТЕХНОГЕННА БЕЗПЕКА

Техногенна безпека – це комплекс заходів і дій, спрямованих на запобігання аваріям і катастрофам на об'єктах техногенної діяльності, а також на мінімізацію наслідків таких подій для людей, довкілля та матеріальних цінностей. Техногенна безпека охоплює заходи щодо попередження, ліквідації та мінімізації наслідків техногенних аварій, інцидентів і катастроф. Техногенна безпека є складним соціальним та економічним явищем, яке охоплює різноманітні аспекти захисту людства та природного середовища від негативних наслідків техногенної діяльності. Техногенна безпека тісно пов'язана з науково-технічним прогресом і рівнем індустріалізації суспільства. З одного боку, розвиток технологій та індустрії сприяє економічному зростанню, підвищенню якості життя та розширенню можливостей людства. З іншого боку,

неконтрольоване використання технологій та індустріальних процесів може призводити до серйозних загроз для здоров'я людини, довкілля та економічної стабільності.

Основні аспекти техногенної безпеки включають: 1) Соціальні аспекти; вплив техногенних ризиків на здоров'я та життя людей; соціальна відповідальність за техногенні катастрофи та аварії; питання інформування суспільства про техногенні загрози та заходи їх попередження; освіта та підготовка населення до дій у випадку техногенних аварій. 2) Економічні аспекти: витрати на запобігання та ліквідацію наслідків техногенних катастроф; економічні втрати, пов'язані з простоєм підприємств, пошкодженням інфраструктури, втратами у виробництві та зниженням продуктивності праці; інвестиції в технології та інновації для підвищення техногенної безпеки; економічна ефективність заходів із зниження техногенних ризиків. 3) Екологічні аспекти: вплив техногенних процесів на довкілля, зокрема забруднення повітря, води та ґрунтів; вплив техногенних катастроф на біорізноманіття та екосистеми; необхідність інтеграції екологічних стандартів у виробничі процеси для мінімізації негативного впливу на навколишнє середовище. 4) Правові та регуляторні аспекти: законодавча база для забезпечення техногенної безпеки; роль держави у контролі та нагляді за дотриманням норм техногенної безпеки; міжнародне співробітництво у сфері техногенної безпеки.

Техногенна безпека є критично важливою для стабільного розвитку суспільства, оскільки вона забезпечує захист від потенційних катастроф, які можуть мати масштабні соціальні та економічні наслідки. Її забезпечення вимагає комплексного підходу, що включає наукові дослідження, технологічні інновації, ефективне управління ризиками, а також активну участь суспільства. Країни повинні приділити пильну увагу побудові інформатизації управління надзвичайними ситуаціями. Були досягнуті прориви у створенні «розумної» платформи великих даних, для яких слід віднести: 1) інтегроване управління, екстрений зв'язок, глобальна поінформованість, короткострокове попередження та збирання даних, що допоможе сформувати систему управління надзвичайними ситуаціями під час стихійних лих, систему моніторингу та раннього попередження про небезпечні хімікати, будівництва «розумних надзвичайних ситуацій».

Керівники підприємств, уряди повинні приділяти пильну увагу інноваціям у сфері запобігання, реагування та порятунку під час аварії та катастроф, упровадженню інновацій у короткостроковому попередженні у разі стихійних лих. Проводити оглядові навчання з аварій і катастроф, що сталися в країні і за кордоном, проводити настільне моделювання + практичні навчання з запобігання лісовим пожежам, запобіганню повеней

і запобіганню тайфунів, геологічних катастроф на залізницях, запобіганню небезпечних хімічних ризиків, покращити можливості реагування на надзвичайні ситуації. Виконувати важливі обов'язки щодо запобігання та усунення великих ризиків, оперативно усувати різні аварії та катастрофи, а також виконувати важливу місію із захисту життя та майна людей та підтримання соціальної стабільності, щоб допоможіть побудувати більш високий рівень.

Необхідно дотримуватися підходу, орієнтованого на людину, щоб модернізувати систему та можливості управління надзвичайними ситуаціями. Дотримуватися верховенства людини і життя, твердо утверджувати концепцію безпечного розвитку, завжди ставити безпеку життя людей на перше місце, упроваджувати концепцію, згідно з якою розвиток не повинен здійснюватися за рахунок людського життя. Щоб задовольнити нові вимоги підприємств, необхідно удосконалювати системи та механізми запобігання та усунення ризиків, постійно підвищувати здатність реагувати на надзвичайні ситуації в суспільстві та постійно зміцнити здатність боротися зі стихійними лихами, щоб забезпечити ефективніші гарантії безпеки та розвитку.

Профілактика повинна вважатися пріоритетом і прагнути запобігати та усувати основні ризики для безпеки. Це є основною функцією управління надзвичайними ситуаціями. Ми наполягаємо на систематичному мисленні, наполягаємо на тому, щоб поєднувати профілактику з порятунком, упроваджувати «запобіжні заходи» та ефективно поєднувати «людський захист», «фізичний захист», «технічний захист» і «контрольний захист».

Керівники підприємств повинні зміцнити спільні сили «людського захисту», закласти міцну основу «фізичного захисту», підвищити рівень «технічного захисту», покращити заходи «контролю та захисту», побудувати «захисну стіну» для запобігання безпеці. Повністю усвідомлювати характеристики та закономірності загроз безпеці, реагувати на малоймовірні події, використовуючи системне мислення, всебічно досліджувати ризики, виявляти основні ризики та ефективно їх усувати. Необхідно провести поглиблений аналіз та оцінку можливого впливу заходів щодо запобігання та контролю епідемій усередині країни, змін в економічній ситуації на безпеку виробництва, запобігання, скорочення та надання допомоги при стихійних лихах.

Техногенна безпека є важливим аспектом національної безпеки, що забезпечує захист людей, майна та навколишнього середовища від негативних наслідків техногенної діяльності. Вона вимагає системного підходу та постійного вдосконалення з урахуванням новітніх технологій та світового досвіду.

Таблиця 9.22 – Основні компоненти техногенної безпеки

Ключовий компонент	Зміст та характеристика
1	2
Промислові аварії	Розробка та впровадження систем безпеки на підприємствах для запобігання вибухам, пожежам, витокам небезпечних речовин, зокрема на хімічних, нафтохімічних, металургійних, енергетичних підприємствах.
Енергетична безпека	Забезпечення безпеки енергетичних об'єктів, таких як електростанції, атомні електростанції, трансформаторні підстанції, для запобігання аварій, що можуть призвести до масштабних відключень електропостачання або радіаційного забруднення.
Техногенна безпека транспорту	Запобігання аваріям на залізничному, авіаційному, автомобільному та морському транспорті шляхом удосконалення систем управління, контролю за станом транспортних засобів і інфраструктури.
Аналіз і оцінка ризиків	Проведення систематичного аналізу можливих техногенних загроз та оцінка ризиків на об'єктах підвищеної небезпеки. Визначення можливих сценаріїв розвитку аварій та їх наслідків.
Системи моніторингу та контролю	Впровадження автоматизованих систем моніторингу, які контролюють критичні параметри на виробничих об'єктах і інформують про можливі відхилення від норми, що можуть призвести до аварії.
Підготовка до аварійних ситуацій	Проведення навчань і тренувань для персоналу підприємств з відпрацювання дій у разі виникнення аварійних ситуацій. Розробка та впровадження інструкцій з безпеки та аварійних планів.
Освіта і підвищення кваліфікації	Організація навчальних програм з техногенної безпеки для підготовки фахівців, що працюють на об'єктах підвищеної небезпеки.
Системи захисту	Впровадження технічних засобів і систем захисту, таких як протипожежні системи, системи автоматичного вимкнення, системи безпеки виробничих процесів, резервні системи живлення.
Підтримка в належному стані технічних засобів	Регулярна перевірка і технічне обслуговування обладнання, систем захисту, інфраструктури для забезпечення їхньої надійності та запобігання аваріям.
Аварійно-рятувальні служби	Організація і підготовка спеціалізованих служб для швидкого реагування на техногенні аварії, проведення рятувальних робіт, евакуація населення, надання першої медичної допомоги.
Дегазація та деконтамінація	Проведення заходів з очищення територій, водних об'єктів та повітря від шкідливих і небезпечних речовин, які можуть бути викинуті в навколишнє середовище внаслідок техногенних аварій.

Закінчення таблиці 9.22

1	2
Запобігання забрудненню довкілля	Впровадження екологічно безпечних технологій і заходів з утилізації відходів, запобігання викидам шкідливих речовин в атмосферу, ґрунт і водні об'єкти.
Відновлення навколишнього середовища	Організація робіт з відновлення екосистем після техногенних катастроф, таких як розливи нафти, хімічне забруднення, радіаційне зараження.
Інформування населення	Надання достовірної інформації про техногенні загрози, можливі наслідки аварій та заходи безпеки. Це включає оповіщення населення, інформування через засоби масової інформації.
Законодавче регулювання	Розробка і впровадження нормативно-правової бази, що регулює діяльність у сфері техногенної безпеки. Це включає закони, постанови, інструкції, що визначають обов'язки суб'єктів господарювання, державних органів і населення.
Обмін досвідом і технологіями:	Співпраця з міжнародними організаціями, обмін досвідом і передовими практиками в галузі техногенної безпеки. Використання міжнародних стандартів і рекомендацій.
Міжнародна допомога в разі катастроф	Координація з іншими країнами і міжнародними організаціями для надання гуманітарної допомоги та технічної підтримки під час ліквідації наслідків великих техногенних катастроф.

Катастрофи – це раптові, катастрофічні події, які спричиняють значні руйнування, збитки та втрати. Загалом вони поділяються на дві групи: природні та техногенні. До природних катастроф належать урагани, землетруси, повені та цунамі. Тим часом, техногенні катастрофи охоплюють такі події, як ядерні аварії, терористичні атаки та розливи нафти. Для довгострокової стабільності країни управління стихійними лихами має першорядне значення. Воно зміцнює стійкість, гарантуючи швидке відновлення співтовариств після стихійного лиха. Крім того, пріоритет управління стихійними лихами забезпечує стійкий розвиток, закладаючи основу для безпечного, процвітаючого майбутнього. За ці роки технології змінили управління стихійними лихами. Тепер безпілотники обстежать райони, що постраждали від стихійних лих, а системи раннього оповіщення допомагають запобігати катастрофам. Розвиток аналітики даних та штучного інтелекту ще більше допомагає у прогнозуванні та реагуванні, роблячи втручання своєчасними та більш ефективними. Технології сьогодні відіграють ключову роль у створенні систем раннього оповіщення про цілу низку катастроф. Для землетрусів використовують сейсмографи для виявлення поштовхів. Супутники та гідрологічні моделі допомагають передбачати повені, а метеорологічні дані прогнозують циклони задовго до їхнього настання.

Приведемо приклади успішного застосування систем раннього оповіщення: 1) Система оповіщення про землетруси в Японії виділяється тим, що попереджає про підземні поштовхи за секунди чи хвилини, рятуючи життя та інфраструктуру. 2) Система сповіщення про циклони у Бангладеш значно знизила кількість жертв за рахунок забезпечення своєчасної евакуації. 3) У Європі Європейська система оповіщення про повені (EFAS) пропонує ранні прогнози повеней, допомагаючи швидко реагувати та пом'якшувати наслідки. Створення систем раннього оповіщення не обходиться без проблем. Забезпечення точних прогнозів, управління високими витратами на встановлення та створення суспільної поінформованості можуть бути лякаючими. Проте міжнародне співробітництво, інвестиції в дослідження та освіту на рівні спільнот можуть прокласти шлях до більш ефективних та поширених систем оповіщення. Використання дистанційного зондування у боротьбі зі стихійними лихами виступає однією з технологій. Дистанційне зондування виступає пріоритетною технологією у моніторингу та оцінці катастроф. Супутники та безпілотники збирають дані в режимі реального часу, надаючи безцінну інформацію про масштаби та розвиток катастроф.

ГІС (географічні інформаційні системи) також активно використовуються в управлінні стихійними лихами. Її додатки оптимізують готовність до стихійних лих, організують швидке реагування та забезпечують ефективні зусилля щодо відновлення шляхом картування постраждалих територій та ресурсів. Минулі катастрофи свідчать про потужність цих технологій. Супутникові знімки під час цунамі в Індійському океані 2004 деталізували зміни узбережжя, сприяючи ефективної допомоги. Аналогічно, дані ГІС після урагану Катріна у 2005 році відіграли важливу роль у визначенні затоплених регіонів та ефективному напрямку допомоги. Велику роль сьогодні відіграє глибоке занурення у великі дані та потенціал ШІ у реагуванні на стихійні лиха. Аналітика великих даних та ШІ не просто покращують операції з реагування на стихійні лиха; вони їх революціонізують. Використовуючи різноманітні набори даних – від соціальних мереж до метеорологічних даних – ці технології виявляють аномалії та потенційні загрози ще до того, як вони загостряться. Штучний інтелект, особливо машинне навчання, стає дедалі більш значущим у сфері зниження ризику лих. Його функції включають прогнозування екстремальних подій, створення карт небезпек, виявлення подій у реальному часі, надання ситуаційної обізнаності, допомога у прийнятті рішень та багато іншого.

Таблиця 9.23 – Напрями запобігання техногенним аваріям та катастрофам

Напрям	Умови реалізації
1	2
Аналіз економічних ризиків	Оцінка можливих економічних втрат від техногенних аварій та катастроф, розробка стратегій зниження цих ризиків. Визначення обсягів страхування підприємств і об'єктів підвищеної небезпеки.
Фінансування заходів з техногенної безпеки	Впровадження механізмів фінансування проектів з покращення техногенної безпеки, таких як модернізація обладнання, підвищення кваліфікації персоналу, впровадження нових технологій.
Розвиток резервних фондів	Формування і підтримка державних і приватних резервних фондів для компенсації збитків і фінансування відновлення після техногенних катастроф. Це включає створення запасів матеріальних ресурсів, страхових фондів, фондів для відновлення інфраструктури.
Економічне планування і управління ризиками	Розробка стратегій управління економічними ризиками в умовах техногенних загроз, створення сценаріїв економічного відновлення, стимулювання інновацій у сфері безпеки.
Інноваційні рішення в промисловості	Застосування передових технологій, таких як автоматизація виробничих процесів, інтелектуальні системи моніторингу та управління, для підвищення безпеки на виробництві та зниження ймовірності аварій.
Цифровізація та управління даними	Використання великих даних (Big Data), штучного інтелекту (ШІ), Інтернету речей (IoT) для створення інтегрованих систем управління техногенною безпекою. Це включає розробку моделей прогнозування аварій та оптимізацію реакції на надзвичайні ситуації.
Інвестиції в інновації	Стимулювання інвестицій в інноваційні технології, що сприяють підвищенню техногенної безпеки. Це може включати державні програми підтримки досліджень і розробок у сфері безпеки, гранти на впровадження нових технологій.
Співпраця з науковими та дослідницькими установами	Підтримка партнерства між підприємствами, урядом і науковими установами для розробки та впровадження новітніх рішень у сфері техногенної безпеки.
Стратегічне планування техногенної безпеки	Створення довгострокових стратегій національної техногенної безпеки, що враховують глобальні тенденції, нові виклики та загрози. Розробка планів дій на випадок великих техногенних катастроф, включаючи міжнародну координацію та співпрацю.
Інтеграція техногенної безпеки у державне управління	Включення питань техногенної безпеки в усі рівні державного управління, від національного до місцевого. Це включає створення спеціалізованих органів і комісій, відповідальних за розробку та реалізацію політики техногенної безпеки.
Оцінка ефективності заходів безпеки	Регулярний моніторинг і оцінка ефективності заходів техногенної безпеки, що впроваджуються. Це включає проведення аудиту безпеки, аналіз інцидентів, що відбулися, і корекцію стратегій.

Закінчення таблиці 9.23

1	2
Управління змінами	Впровадження процедур управління змінами, що дозволяють швидко реагувати на нові загрози та виклики, адаптувати плани та стратегії техногенної безпеки до змінних умов.
Визнання та дотримання міжнародних стандартів	Адаптація національних норм і стандартів до міжнародних вимог, забезпечення відповідності стандартів підприємств і організацій міжнародним нормативам.
Глобальні партнерства	Встановлення міжнародних партнерств для обміну досвідом, технологіями та передовими практиками у сфері техногенної безпеки. Це включає укладання міжнародних угод про співпрацю у випадках техногенних катастроф.
Участь у міжнародних навчаннях та тренуваннях	Спільна організація та участь у міжнародних навчаннях, спрямованих на підвищення готовності до реагування на великі техногенні катастрофи. Це дозволяє підвищити рівень підготовки персоналу та удосконалити механізми міжнародної координації.

Техногенна безпека є складним і багатогранним напрямком, що охоплює широкий спектр заходів і стратегій, спрямованих на захист людей, майна і довкілля від негативних наслідків техногенних факторів. Вона вимагає постійного вдосконалення, інновацій і співпраці на всіх рівнях – від місцевого до міжнародного. Окрім базового прогнозування, машинне навчання пропонує складне моделювання катастроф. Воно обробляє десятиліття даних про катастрофи для моделювання сценаріїв, допомагаючи владі підготуватися до раніше немислимих подій. Але справжня геніальність ШІ полягає у його адаптивності. З розвитком ситуацій моделі ШІ коригують свої прогнози, гарантуючи, що стратегії надання допомоги залишаються актуальними. Більше того, обробка природної мови, ще один напрямок ШІ, тепер сканує соціальні мережі в режимі реального часу під час катастроф. Це забезпечує оновлення з нуля, дозволяючи швидше реагувати на загрози або прохання про допомогу, що виникають. При плануванні надзвичайних ситуацій ШІ це не просто інструмент, моделювання на основі ШІ спрямовує стратегію, панелі управління на основі даних допомагають контролювати розподіл ресурсів, автоматизація прискорює виконання трудомістких завдань. Завдяки цим досягненням ми стаємо свідками світанку нової ери у реагуванні на стихійні лиха та готовність до них.

Розширення можливостей ліквідації наслідків стихійного лиха відбувається за допомогою комунікаційних технологій. Ефективна комунікація під час катастроф – це рятівне коло. Вона з'єднує застряглих, інформує стривожених та координує рятувальників, часто визначаючи різницю між життям та смертю. Впроваджуються сучасні комунікаційні технології. Супутникові

телефони кидають виклик традиційним мережевим проблемам, гарантуючи, що рятувальники залишаються на зв'язку у найвіддаленіших місцях. Соціальні мережі діють як маяк, транслюючи повідомлення SOS та оновлення урежимі реального часу, мобілізуючи глобальну підтримку. Мобільні програми, адаптовані для сценаріїв катастроф, допомагають у відстеженні, розподілі ресурсів і навіть у наданні першої медичної допомоги.

Таблиця 9.24 – Приклади позитивного досвіду у вирішенні проблем техногенної безпеки

Країна	Позитивний досвід вирішення техногенної катастрофи
Україна: Чорнобильська катастрофа та зона відчуження	Після аварії на Чорнобильській АЕС у 1986 році, Україна та міжнародна спільнота провели значну роботу для забезпечення техногенної безпеки. Зона відчуження навколо ЧАЕС стала прикладом масштабного проекту з мінімізації радіаційного впливу на людей та довкілля. Успішно проведена операція зі зведення нового саркофага над реактором у 2016 році є прикладом ефективної міжнародної співпраці та впровадження сучасних технологій для підвищення безпеки.
Японія: управління наслідками аварії на Фукусімській АЕС	У 2011 році після землетрусу та цунамі, які викликали аварію на Фукусімській АЕС, Японія впровадила низку заходів для подолання наслідків техногенної катастрофи. Включені в це заходи моніторинг радіоактивного забруднення, евакуація населення та очищення територій. Успіх цих заходів демонструє важливість швидкого реагування, інноваційних підходів та залучення громадськості до процесу відновлення.
США: система попередження та реагування на аварії на хімічних підприємствах	Після серії хімічних катастроф у США, таких як аварія на Union Carbide в Індії (Бхопал), було прийнято низку законів і стандартів, спрямованих на покращення техногенної безпеки. Впровадження системи попередження аварій та оперативного реагування, включаючи систему EPCRA (Emergency Planning and Community Right-to-Know Act), допомогло значно знизити кількість інцидентів на хімічних підприємствах.
Європейський Союз: Директива Seveso	Після аварії на хімічному заводі в Севезо, Італія, у 1976 році, Європейський Союз запровадив директиву Seveso, що встановила суворі вимоги до управління техногенною безпекою на промислових об'єктах, які працюють з небезпечними речовинами. Ця директива забезпечує надійний контроль за ризиками, зокрема через обов'язкове планування та підготовку до надзвичайних ситуацій, що значно підвищує рівень безпеки на європейських підприємствах.
Швеція: комплексний підхід до управління безпекою на атомних електростанціях	У Швеції успішно впроваджено систему багаторівневого контролю та захисту на атомних електростанціях. Це включає регулярне тестування безпеки, модернізацію технологій, а також активну участь у міжнародних обмінах досвідом. Такий підхід дозволив Швеції досягти одного з найвищих рівнів безпеки в галузі атомної енергетики.

Ці приклади показують, що при належному плануванні, сучасних технологіях і міжнародній співпраці можна успішно вирішувати складні питання техногенної безпеки.

Інформаційно-комунікаційні технології (ІКТ) відіграють ключову роль у створенні мережевої допомоги. Безшовно пов'язуючи постраждалі спільноти з агентствами з надання допомоги, ІКТ гарантує, що допомога не просто в дорозі, а на правильному шляху, досягаючи тих, хто її найбільше потребує. Завдяки технологіям реакція людства на загрози природи стає швидшою, розумнішою та співчутливішою. Дрони та робототехніка – це майбутнє відновлення після стихійного лиха. Безпілотники виявляються безцінними у ліквідації наслідків катастроф. Завдяки можливості швидко обстежити великі території, вони стали ключовими гравцями в оцінці збитків та пошуково-рятувальних операціях, знімаючи в реальному часі кадри з повітря, що прискорює час реагування. На складних ділянках та в небезпечних умовах роботи займають центральне місце. Будь то переміщення по руїнах після землетрусу або проникнення в радіоактивні зони, робототехніка забезпечує безпеку, водночас допомагаючи у критично важливих відновлювальних роботах.

Кібербезпека виступає як основа ефективного управління стихійними лихами. Сьогоднішній взаємопов'язаний світ посилює важливість кібербезпеки в управлінні катастрофами. Критична інфраструктура – лікарні, транспорт та мережі зв'язку – все більше покладається на цифрові системи. Кіберзлом під час катастрофи може спричинити подвійну небезпеку, загальмувати реагування та посилити кризи. Надзвичайні ситуації можуть стати золотою жилою для зловмисних кіберзлочинців. Коли відвертається увага, вони можуть почати атаки, поширювати дезінформацію або скомпрометувати основні служби. Наприклад, під час атаки вірусу-здирника WannaCry у 2017 році було порушено такі критично важливі служби, як заклади охорони здоров'я у Великій Британії, що підкреслює зв'язок між кібербезпекою та громадською безпекою.

Встановлюючи надійні протоколи кібербезпеки, агенції з управління стихійними лихами зміцнюють свою здатність підтримувати зв'язок, захищати конфіденційну інформацію та ефективно розподіляти ресурси. Цей проактивний підхід гарантує, що при виникненні стихійного лиха системи на місці залишаться стійкими, зберігаючи здатність пом'якшувати наслідки, реагувати та відновлюватися, не піддаючись додатковим викликам кіберзагроз. Приведемо приклади з практики історії успіху управління стихійними лихами. Після руйнівного землетрусу 2010 року Гаїті зіткнулася з величезними труднощами у збиранні точних даних для координації зусиль з надання допомоги. Використання технологій, зокрема мобільних телефонів, відіграло

вирішальну роль у цьому сценарії. Такі організації, як Ushahidi, використовували краудсорсинг для складання карти районів, які потребують допомоги, за допомогою SMS та повідомлень у соціальних мережах. Цей технологічний підхід дозволив рятувальникам ефективно спрямовувати допомогу, гарантуючи, що ресурси будуть доставлені у потрібні місця.

Управління повенями в Індії за допомогою дистанційного зондування. Досвід Індії у боротьбі з повенями, викликаними мусонами, привів до ухвалення йдистанційного зондування. Використовуючи супутникові дані, прогнози погоди та географічні інформаційні системи (ГІС), уряд може прогнозувати регіони, що зазнають повеней, та планувати стратегії евакуації. Наприклад, під час повеней у Кералі у 2018 році дистанційне зондування дозволило здійснювати моніторинг рівня води у режимі реального часу, що допомогло рятувальним операціям та розподілу ресурсів.

Проєкти сейсмостійких будівель у Чилі: Чилі, розташована вздовж Тихоокеанського вогняного кільця, інтегрувала технології в архітектурні практики для стійкості до стихійних лих. Передові інженерні технології, включно з проєктами сейсмостійких будівель, значно скоротили кількість жертв під час землетрусів. Встановлення датчиків у будинках допомагає виявляти структурні слабкості, що дозволяє проводити своєчасний ремонт для запобігання потенційним обваленням. У цих випадках технології довели свою ефективність в управлінні надзвичайними ситуаціями та реагуванні на них, продемонструвавши силу інновацій у порятунку життів та мінімізації наслідків стихійного лиха.

Політика та управління для управління катастрофами на основі технологій – це формування стійкого майбутнього. Налаштування обстановки за допомогою політик та фінансових стимулів: урядова політика може виступати як дороговказ. Визначаючи чіткі стандарти та рамки, вони забезпечують дорожню карту для інтеграції технологій у стратегію управління катастрофами. Уряди можуть сприяти впровадженню технологій, пропонуючи податкові пільги, гранти або фінансування організаціям чи стартапам, зосередженими на рішеннях боротьби з катастрофами на основі технологій. Ефективне управління стихійними лихами – це не одиночна акція; це злагоджена співпраця державних установ, приватного сектору та громадянського суспільства. Державні агентства закладають основу, забезпечуючи інфраструктурну та логістичну підтримку, вониможуть запропонувати ресурси, персонал і, що найважливіше, нормативну базу, яка дозволяє об'єднатися. Інновації – сильна сторона приватного сектору – від дронів, які надають гуманітарну допомогу, до аналітики на основі штучного інтелекту, яка прогнозує катастрофи, приватний сектор привносить рішення, які можна масштабувати та вдосконалювати.

Громадянське суспільство: низові організації, НУО та громадські групи відіграють вирішальну роль у подоланні розриву між технологіями та їх кінцевими користувачами. Вони можуть допомогти адаптувати технічні рішення на основі місцевих потреб, гарантуючи, що вони будуть як ефективними, так і культурно значущими. Ключовим моментом є відкрита комунікація. Регулярні діалоги, семінари та спільні ініціативи можуть сприяти створенню середовища, в якому знання та ресурси обмінюються, що призводить до комплексних рішень щодо управління катастрофами.

Подолання труднощів у технологічному управлінні стихійними лихами – це шлях до технологічно орієнтованого управління катастрофами, який не позбавлений перешкод. Усвідомлення цих проблем – перший крок до їх вирішення: 1) Фінансові обмеження: хоча технології обіцяють ефективність, вони мають свою ціну. Обмежені бюджети часто можуть перешкоджати повномасштабному впровадженню передових технологічних рішень. 2) Технічні знання: не кожен спеціаліст з управління стихійними лихами розуміється на технологіях. Пробіл у технічних знаннях може призвести до недовикористання або навіть неправильного використання наявних інструментів. 3) Культурний опір: у багатьох регіонах існує вроджена довіра та розроблена система управління катастрофами. Впровадження технологій може зустріти опір, оскільки вони вважаються руйнівними чи неперевіреними. Подолання цих проблем потребує проактивного підходу. Постійне навчання, пілотування нових технологій, виділення коштів на дослідження та розробки, а також заохочення культури відкритості до інновацій – лише кілька способів забезпечити процвітання ініціатив з управління стихійними лихами, заснованих на технологіях.

Шлях до майбутнього, стійкого до катастроф, детермінується технологічними інноваціями. Оскільки ми стоїмо на порозі цифрового нового світу, наша колективна відповідальність – розумно використовувати ці інструменти, завжди прагнучи безпечнішої, більш підготовленої технологічної безпеки. Для цього слід дотримуватись інноваційного мислення та продовжувати просувати інновації у системах та механізмах управління надзвичайними ситуаціями, щоб інновації були головною рушійною силою і повною мірою використовували механізм реформ та інновацій.

Впроваджувати інновації у вдосконаленні комплексного механізму координації, дотримуватись принципу «оптимізації, координації та ефективності» для подальшого вдосконалення управління надзвичайними ситуаціями. Впроваджувати інновації у створенні механізму підготовки кадрів для управління надзвичайними ситуаціями, активно розвивати таланти та зміцнювати створення дисциплін управління надзвичайними ситуаціями. Досягати інновацій у побудові інформатизації, наполягати

на відкритті дверей для інновацій, зміцнювати інтегроване командування, короткострокове раннє попередження, глобальну поінформованість та дані. Інтелектуальна інформатизація управління надзвичайними ситуаціями дозволить всебічно покращити рівень цифрової інформатизації та інтелекту управління надзвичайними ситуаціями, сприятиме модернізації управління надзвичайними ситуаціями за допомогою інтелекту. сприяти модернізації систем та можливостей управління надзвичайними ситуаціями. реалізація великих інженерних проектів. Удосконалення системи відповідальності за безпеку виробництва. Керівники підприємств наполягають на виділенні ключових напрямків, ключових періодів та ключових вузлів, особливому забезпеченню ключових галузей, таких як небезпечні хімічні речовини, автомобільний транспорт, будівництво, рибальські судна та пожежна безпека. Керівники підприємств наполягають на проблемній орієнтації, продовжують впроваджувати інновації у робочий механізм безпеки виробництва та активно запускають низку практичних та жорстких заходів щодо безпеки виробництва спільно з відповідними відомствами, завжди дотримуватися розвитку та ніколи не жертвувати людським життям, публічно попереджати про великі ризики, створили систему управління інформацією про джерела небезпе, посилиди практичні та жорсткі заходи щодо безпечного виробництва, оперативно активувати механізм реагування на надзвичайні ситуації.

Теоретичне значення вирішення техногенної безпеки полягає у формуванні наукових підходів, концепцій та моделей, що дозволяють глибше розуміти та аналізувати ризики, пов'язані з техногенними катастрофами та надзвичайними ситуаціями. Це включає розвиток теорій управління ризиками, прогнозування наслідків техногенних аварій, аналізу впливу технологій на безпеку, а також створення науково обґрунтованих методів запобігання та мінімізації негативних наслідків. Практичне значення вирішення питань техногенної безпеки полягає в розробці та впровадженні конкретних заходів, спрямованих на захист людей, інфраструктури та довкілля від негативних наслідків техногенних катастроф. Це включає: розробку нормативних актів і стандартів, що регулюють безпечну експлуатацію технічних систем і об'єктів; впровадження сучасних технологій моніторингу та попередження аварій, таких як системи раннього виявлення ризиків і аварійних ситуацій; навчання та підготовку персоналу, здатного ефективно діяти в умовах надзвичайних ситуацій; планування заходів із ліквідації наслідків катастроф і мінімізації збитків, що включає організацію евакуації, надання першої допомоги та відновлення інфраструктури; створення інфраструктури для оперативного реагування на техногенні катастрофи, включаючи рятувальні служби, медичні підрозділи та інші необхідні ресурси.

Таким чином, вирішення питань техногенної безпеки має важливе значення як у теоретичній площині, формуючи основи для подальших досліджень та інновацій, так і в практичній, забезпечуючи захист суспільства від загроз, пов'язаних з технологічним прогресом.

9.5 ВИРОБНИЧА БЕЗПЕКА ТА БЕЗПЕКА ПРАЦІ

Виробнича безпека – це комплекс заходів, спрямованих на забезпечення безпечних умов праці, захист життя та здоров'я працівників, а також на попередження травматизму та аварій на виробництві, запобігання нещасним випадкам, травмам, працівників від потенційних небезпек, пов'язаних з їх професійною діяльністю. Вона охоплює всі аспекти виробничого процесу, включаючи технічне обладнання, організацію праці, санітарно-гігієнічні умови та навчання персоналу. Безпека праці є важливим аспектом будь-якого суспільства, оскільки забезпечення безпечних умов праці має прямий вплив на загальну цивільну безпеку. Безпека праці включає в себе комплекс заходів, спрямованих на захист працівників від виробничих ризиків, що можуть призвести до травм, захворювань або інших небажаних наслідків. У свою чергу, цивільна безпека залежить від ефективної реалізації цих заходів на рівні підприємств, організацій та держави загалом. Безпека праці тісно пов'язана з соціальною стабільністю в суспільстві. Небезпечні умови праці можуть призводити до підвищеного рівня травматизму, професійних захворювань та загальної незадоволеності працівників, що створює ризики соціальних конфліктів. У свою чергу, високий рівень безпеки праці сприяє зменшенню соціальної напруги, підвищенню довіри працівників до роботодавців і держави, що є важливим чинником стабільності в суспільстві.

Виробнича безпека забезпечує збереження життя та здоров'я працівників, підвищення продуктивності праці, а також мінімізацію ризиків для підприємства та довкілля. Застосування сучасних технологій, таких як автоматизація, робототехніка, і штучний інтелект, сприяє підвищенню рівня виробничої безпеки. Автоматизовані системи можуть виконувати небезпечні завдання замість людей, знижуючи ризики травм. Крім того, технології можуть бути використані для моніторингу умов праці в режимі реального часу, швидкого виявлення небезпечних ситуацій та своєчасного реагування на них. Ефективний менеджмент є ключовим фактором у забезпеченні виробничої безпеки. Керівництво повинно не лише встановлювати стандарти безпеки, але й забезпечувати їхнє дотримання на всіх рівнях організації. Це включає проведення регулярних перевірок,

заохочення культури безпеки серед працівників, а також швидке реагування на будь-які порушення або інциденти. Виробнича безпека має також соціальний вимір, оскільки забезпечення безпечних умов праці позитивно впливає на соціальний клімат у колективі, зменшує плинність кадрів і підвищує мотивацію працівників. Робітники, які почуваються захищеними на своєму робочому місці, більш задоволені своєю роботою і готові ефективніше виконувати свої обов'язки. Для забезпечення високого рівня виробничої безпеки підприємства проводять регулярні аудити та отримують сертифікацію за міжнародними стандартами, такими як OHSAS 18001 або ISO 45001. Це підтверджує відповідність системи безпеки на підприємстві найкращим світовим практикам і сприяє підвищенню довіри з боку працівників, партнерів і клієнтів. Важливим аспектом є інвестування у безпеку праці. Це включає модернізацію обладнання, впровадження нових технологій, навчання персоналу, покращення умов праці та забезпечення працівників належними засобами захисту. Інвестиції в безпеку є довгостроковими, але вони окуповуються за рахунок зниження витрат на ліквідацію аварій, компенсації та підвищення ефективності виробництва. Виробнича безпека є глобальним питанням, і міжнародне співробітництво в цій сфері сприяє поширенню найкращих практик та стандартів. Обмін досвідом, участь у міжнародних конференціях і співпраця з міжнародними організаціями, такими як Міжнародна організація праці (МОП), допомагає підприємствам удосконалювати свої системи безпеки.

Таким чином, виробнича безпека є багатогранною концепцією, яка охоплює різні аспекти діяльності підприємства. Її впровадження забезпечує захист здоров'я і життя працівників, підвищення ефективності виробництва, зниження економічних ризиків та підтримку соціальної стабільності.

Таблиця 9.25 – Основні компненти виробничої безпеки

Виклики та загрози	**Зміст та характеристика**
1	2
Безпека та охорона праці	Впровадження заходів для захисту здоров'я і життя працівників, включаючи дотримання стандартів безпеки, забезпечення відповідних умов праці та попередження професійних захворювань. Розробка і впровадження систем управління охороною праці, що включають аналіз ризиків, планування заходів безпеки, моніторинг і оцінку ефективності впроваджених заходів.
Безпека обладнання та технологічних процесів	Забезпечення справності обладнання, його відповідність стандартам безпеки, проведення регулярних технічних оглядів та обслуговування. Впровадження систем автоматичного контролю і управління технологічними процесами, що знижують ризики аварійних ситуацій.

Продовження таблиці 9.25

1	2
Розробка і впровадження інструкцій з безпеки	Створення і дотримання інструкцій з безпеки на робочих місцях, проведення інструктажів для працівників щодо правил безпеки. Планування робочих місць з урахуванням ергономіки, оптимізації умов праці, запобігання небезпечним ситуаціям.
Санітарно-гігієнічні умови	Контроль за умовами праці, включаючи освітлення, вентиляцію, рівень шуму, температурний режим та інші фактори, що впливають на здоров'я працівників. Надання працівникам необхідних засобів захисту (каски, рукавички, маски, спецодяг) для запобігання травмам та впливу шкідливих факторів.
Навчання правилам безпеки	Проведення регулярних навчальних курсів, тренінгів і інструктажів для працівників з питань безпеки на виробництві. Створення програм з підвищення кваліфікації працівників, зокрема з безпеки праці, для запобігання нещасним випадкам і підвищення ефективності роботи.
Планування дій на випадок аварій	Розробка і впровадження планів евакуації, аварійних інструкцій, процедур реагування на надзвичайні ситуації. Організація аварійно-рятувальних підрозділів: Створення і підтримка аварійно-рятувальних підрозділів, які мають відповідні знання і технічні засоби для швидкого реагування на аварійні ситуації.
Психологічна безпека	Забезпечення психологічної підтримки працівників, створення сприятливого робочого середовища, яке знижує рівень стресу і підвищує мотивацію. Надання психологічних консультацій та підтримки працівникам, особливо після виникнення стресових або аварійних ситуацій.
Моніторинг і аудит виробничої безпеки:	Проведення постійного моніторингу умов праці для виявлення потенційних ризиків і небезпек, своєчасне їх усунення. Здійснення незалежних аудитів і перевірок виробничих умов, оцінка ефективності системи безпеки на підприємстві.
Правова підтримка і регулювання	Забезпечення відповідності виробничої діяльності всім чинним законам і нормативним актам у сфері безпеки праці. Гарантії прав працівників на безпечні умови праці, можливість звернення до суду у випадку порушення цих прав.
Інтеграція виробничої безпеки у бізнес-процеси	Інтеграція питань безпеки праці у всі бізнес-процеси підприємства, від планування до виробничих операцій. Впровадження міжнародних стандартів, таких як ISO 45001, що стосуються системи управління охороною праці та забезпечення безпеки.
Забезпечення соціальної відповідальності бізнесу	Реалізація програм соціальної відповідальності, спрямованих на покращення умов праці, розвиток культури безпеки на виробництві. Підготовка і публікація звітів про стан безпеки праці, проведення діалогу з працівниками та зацікавленими сторонами щодо покращення умов праці.

Закінчення таблиці 9.25

1	2
Оцінка ризиків та аварійне реагування	Виявлення і оцінка потенційних небезпек на робочому місці та підготовка планів і процедур на випадок виникнення надзвичайних ситуацій на виробництві.
Дотримання нормативних вимог та розробка та впровадження захисних заходів	Виконання національних і міжнародних стандартів безпеки праці та встановлення інженерних бар'єрів, використання засобів індивідуального захисту (ЗІЗ), навчання працівників безпечним методам роботи.
Контроль і моніторинг та навчання персоналу	Регулярні перевірки, аудит безпеки, моніторинг виконання безпекових процедур. Проведення інструктажів, тренінгів і навчальних програм для підвищення обізнаності працівників щодо виробничої безпеки.

Виробнича безпека є ключовим аспектом успішної та безперебійної діяльності підприємства, адже вона не лише захищає життя та здоров'я працівників, а й сприяє підвищенню продуктивності, зниженню виробничих витрат та зміцненню репутації компанії на ринку.

Таблиця 9.26 – Інноваційні підходи до впровадження виробничої безпеки

Підхід	**Напрямок впровадження**
1	2
Впровадження інноваційних технологій	Впровадження автоматизованих систем і роботизованих комплексів, які виконують небезпечні операції замість людей. Це знижує ризики травматизму і покращує загальну безпеку на підприємствах.
Інтелектуальні системи моніторингу	Використання технологій Інтернету речей (IoT), штучного інтелекту (ШІ) та великих даних (Big Data) для створення інтегрованих систем моніторингу, які автоматично виявляють і попереджають небезпечні ситуації на виробництві.
Навчання та підготовка працівників	Використання VR/AR технологій для створення тренінгових симуляцій, які дозволяють працівникам тренуватися у безпечних умовах, імітуючи реальні виробничі процеси та надзвичайні ситуації.
Проектування безпечних робочих місць	Застосування доповненої реальності для аналізу та оптимізації робочих місць, що дозволяє заздалегідь виявляти і усувати потенційні небезпеки.
Енергоефективність і зниження шкідливих викидів	Впровадження енергоефективних технологій та методів зниження викидів шкідливих речовин у повітря, що сприяє зменшенню екологічного впливу виробничої діяльності на навколишнє середовище і покращує умови праці.

Закінчення таблиці 9.26

1	2
Переробка відходів і впровадження циркулярної економіки	Використання принципів циркулярної економіки для зменшення кількості виробничих відходів і їх повторного використання, що підвищує загальну безпеку і ефективність виробництва.
Цифровізація управління безпекою:	Впровадження цифрових платформ, що дозволяють централізовано управляти всіма аспектами виробничої безпеки, від моніторингу умов праці до обліку інцидентів і розробки заходів щодо їх усунення.
Аналіз даних і прогнозування ризиків	Використання аналітики великих даних для виявлення трендів і прогнозування потенційних ризиків на виробництві, що дозволяє заздалегідь вживати превентивних заходів.
Освіта і пропаганда безпечних умов праці	Реалізація програм, спрямованих на підвищення обізнаності працівників про важливість дотримання правил безпеки. Це може включати як внутрішньо-корпоративні заходи, так і загальнонаціональні кампанії.
Формування культури безпеки	Створення середовища, де питання безпеки праці є невід'ємною частиною корпоративної культури, і кожен працівник розуміє свою роль і відповідальність за дотримання стандартів безпеки.
Співпраця між працівниками та роботодавцями	Впровадження механізмів соціального партнерства, де працівники і роботодавці спільно розробляють і реалізовують заходи з покращення умов праці та забезпечення безпеки.
Роль профспілок	Активна участь профспілок у забезпеченні виробничої безпеки, включаючи захист прав працівників на безпечні умови праці, контроль за дотриманням стандартів і впровадження нових ініціатив.
Реабілітація та допомога постраждалим	Організація програм реабілітації для працівників, які постраждали внаслідок нещасних випадків на виробництві, включаючи медичну допомогу, психологічну підтримку та допомогу в поверненні до роботи.
Матеріальна допомога та страхування	Надання матеріальної допомоги, включаючи страхові виплати, працівникам і їхнім сім'ям у випадку травм або смерті внаслідок виробничих нещасних випадків.

Забезпечення виробничої безпеки є ключовим завданням для будь-якого підприємства, адже воно не лише захищає життя і здоров'я працівників, але й сприяє підвищенню ефективності виробництва, зниженню витрат на відшкодування збитків і покращенню репутації компанії. Майбутній розвиток виробничої безпеки буде пов'язаний з подальшою автоматизацією, цифровізацією та впровадженням інноваційних технологій, що дозволить

створити ще більш безпечні та ефективні робочі місця. Підвищення культури безпеки, залучення працівників до процесу управління безпекою, розвиток соціального партнерства і впровадження передових технологій – це основні напрямки, які дозволять забезпечити високий рівень безпеки на підприємствах і підвищити загальну якість виробничих процесів.

Цифровізація має значний вплив на виробничу безпеку, змінюючи підходи до управління ризиками, запобігання інцидентам та загалом підвищуючи рівень безпеки на підприємствах.

Таблиця 9.27 – Вплив цифровізації на забезпечення виробничої безпеки

Напрямок впливу	**Зміст та характеристика**
1	2
Автоматизація та роботизація	Цифровізація дозволяє автоматизувати багато виробничих процесів, зменшуючи потребу в людській праці в небезпечних зонах. Роботи та автоматизовані системи можуть виконувати завдання, які пов'язані з високим ризиком, такими як робота в екстремальних температурах, хімічно небезпечних середовищах або в зонах підвищеної радіації. Це значно знижує ризик травматизму серед працівників. Впровадження автоматизованих систем і роботизованих комплексів, які виконують небезпечні операції замість людей. Це знижує ризики травматизму і покращує загальну безпеку на підприємствах.
Інтернет речей (IoT) та підвищений контроль	Інтернет речей дозволяє підключати різні пристрої та системи до єдиної мережі, забезпечуючи постійний моніторинг стану обладнання, умов праці та поведінки працівників. Це дає можливість вчасно виявляти потенційні проблеми та запобігати аваріям. Наприклад, датчики можуть фіксувати перевищення допустимих норм температури, тиску або вібрації, і в разі небезпеки система автоматично зупинить виробничий процес.
Аналіз великих даних (Big Data)	Збір і аналіз великих обсягів даних дозволяє краще розуміти ризики на виробництві. Аналітичні системи можуть прогнозувати можливі інциденти на основі історичних даних, моделювати наслідки різних подій та пропонувати оптимальні рішення для мінімізації ризиків. Це дозволяє перейти від реактивного до проактивного підходу у забезпеченні безпеки праці.
Віртуальна та доповнена реальність (VR/AR)	Віртуальна та доповнена реальність можуть бути використані для навчання працівників безпечним методам роботи в реалістичних, але безпечних умовах. Завдяки VR/AR можна моделювати різні сценарії аварій та навчати персонал правильним діям у надзвичайних ситуаціях. Це значно підвищує підготовленість працівників та знижує ризик помилок.
Покращення комунікації та координації	Цифрові платформи дозволяють покращити координацію між різними підрозділами підприємства, що займаються питаннями безпеки. Завдяки сучасним засобам комунікації інформація про небезпеки, інциденти та заходи реагування може оперативно передаватися всім зацікавленим сторонам. Це забезпечує швидше прийняття рішень та ефективніше реагування на потенційні загрози.

Продовження таблиці 9.27

1	2
Цифрові системи управління безпекою	Інтеграція цифрових систем управління безпекою, таких як ERP (Enterprise Resource Planning) та EHS (Environment, Health, and Safety) системи, дозволяє централізовано керувати всіма аспектами виробничої безпеки. Ці системи можуть автоматизувати процеси, пов'язані з моніторингом, звітністю та дотриманням норм безпеки, що знижує ймовірність людських помилок і підвищує загальну ефективність управління.
Кібербезпека	Цифровізація виробничих процесів робить їх залежними від інформаційних технологій, що, у свою чергу, підвищує ризик кібератак. Захист цифрових систем управління від кіберзагроз стає критично важливим для забезпечення безпеки на виробництві. Порушення роботи IT-систем або несанкціонований доступ до них можуть призвести до серйозних виробничих аварій.
Персоналізація заходів безпеки	Завдяки цифровим технологіям, таким як носимі пристрої (wearables), можна персоналізувати заходи безпеки для кожного працівника. Наприклад, носимі пристрої можуть моніторити фізичний стан працівника (температуру тіла, пульс, рівень стресу) і попереджати про можливе перевтомлення або інші загрози для здоров'я. Це дозволяє забезпечити індивідуальний підхід до безпеки праці.
Підвищення прозорості та звітності	Цифровізація виробничих процесів сприяє підвищенню прозорості та звітності у питаннях безпеки праці. Цифрові системи дозволяють автоматизувати процеси збору та аналізу даних щодо виконання заходів безпеки, інцидентів та їх розслідування. Завдяки цьому керівництво може отримувати точні та своєчасні звіти про стан виробничої безпеки, що сприяє прийняттю обґрунтованих рішень та швидкому реагуванню на порушення.
Інтеграція зі штучним інтелектом (ШІ)	Штучний інтелект відіграє важливу роль у забезпеченні виробничої безпеки, оскільки дозволяє аналізувати великі обсяги даних та виявляти приховані закономірності. Наприклад, ШІ може передбачати ймовірність виникнення нещасних випадків на основі історичних даних, аналізу поведінки працівників та стану обладнання. Це дозволяє запобігти аваріям, вживаючи превентивних заходів ще до того, як виникне реальна небезпека.
Електронні інструкції та навчальні платформи	Цифрові технології сприяють удосконаленню навчання та інструктажу працівників щодо безпеки праці. Електронні інструкції, відеоуроки, симуляції та інтерактивні навчальні платформи дозволяють працівникам ефективніше засвоювати знання про безпечні методи роботи. Цифрові платформи також можуть автоматично відстежувати прогрес навчання та нагадувати про необхідність повторного проходження інструктажів.
Гнучкість та адаптивність виробничих процесів	Цифрові технології забезпечують високу гнучкість та адаптивність виробничих процесів, що дозволяє оперативно реагувати на зміни у виробничому середовищі та умовах праці. Наприклад, у разі виявлення небезпеки цифрова система може автоматично змінити режим роботи обладнання або перенаправити працівників на безпечні ділянки виробництва. Це значно знижує ризик виникнення аварійних ситуацій.

Закінчення таблиці 9.27

1	2
Віддалене управління та контроль	Завдяки цифровізації, керівники та фахівці з безпеки можуть здійснювати віддалене управління та контроль за виробничими процесами. Це особливо актуально для великих підприємств, де виробничі ділянки можуть бути розташовані на великій відстані одна від одної. Віддалений доступ до систем моніторингу та управління безпекою дозволяє швидко виявляти та реагувати на небезпеки, навіть якщо керівник перебуває поза межами виробничого майданчика.
Покращення управління критичними ситуаціями	Цифрові технології сприяють більш ефективному управлінню критичними ситуаціями. Інформаційні системи можуть надавати працівникам точні інструкції у реальному часі, координувати дії різних служб, а також забезпечувати оперативний обмін інформацією між всіма учасниками процесу. Це дозволяє мінімізувати негативні наслідки аварій та інших надзвичайних подій.
Підвищення мотивації та залученості працівників	Цифровізація також може підвищувати мотивацію та залученість працівників у питаннях безпеки. Завдяки використанню інтерактивних платформ та гейміфікації працівники можуть брати активну участь у процесі підвищення рівня безпеки на виробництві, отримувати нагороди за дотримання правил безпеки та досягнення у цій сфері. Це сприяє формуванню культури безпеки на підприємстві та більш відповідальному ставленню працівників до своєї роботи.
Захист навколишнього середовища	Цифрові технології, такі як інтелектуальні системи управління відходами, контроль викидів та енергоефективність, допомагають мінімізувати негативний вплив виробництва на навколишнє середовище. Це не тільки знижує екологічні ризики, але й сприяє дотриманню екологічних норм та стандартів, що, у свою чергу, підвищує загальну виробничу безпеку.
Реалізація концепції Industry 4.0	Цифровізація є основою концепції Industry 4.0, яка передбачає інтеграцію кіберфізичних систем у виробничі процеси. Це дозволяє створювати «розумні» фабрики, де всі компоненти виробничого процесу (від обладнання до людських ресурсів) пов'язані в єдину інформаційну мережу, що сприяє ефективному управлінню безпекою, підвищенню продуктивності та зниженню ризиків.

Цифровізація виробничої безпеки значно підвищує рівень захисту працівників і продуктивність підприємств, а також забезпечує відповідність сучасним вимогам до безпеки та ефективності. Однак вона також вимагає постійного оновлення технологій і навчання персоналу для успішної адаптації до нових умов роботи. Цифровізація відкриває нові можливості для підвищення рівня виробничої безпеки, але також ставить нові виклики, пов'язані з кібербезпекою та адаптацією до технологічних змін. Проте, в загальному, впровадження цифрових технологій значно підвищує ефективність і надійність систем. Цифровізація має суттєвий вплив на охорону праці, покращуючи умови праці, підвищуючи безпеку працівників та оптимізуючи управлінські процеси. Приведемо напрями впливу цифровізації на охорону праці.

Таблиця 9.28 – Напрями впливу цифровізації на охорону праці

Напрямок впливу	Зміст та характеристика впливу цифровізації на охорону праці
Моніторинг умов праці в режимі реального часу	Цифрові технології, такі як Інтернет речей (IoT), дозволяють здійснювати постійний моніторинг умов праці в реальному часі. Датчики можуть відстежувати рівень освітлення, температури, вологості, наявність шкідливих речовин у повітрі тощо. У разі перевищення допустимих норм система може автоматично попереджати працівників або керівництво про небезпеку та вживати відповідних заходів.
Цифрове навчання та інструктажі	Цифрові платформи надають можливість інтерактивного навчання працівників з охорони праці. Віртуальна та доповнена реальність (VR/AR) дозволяють моделювати небезпечні ситуації та навчати працівників правильних дій у таких умовах. Це сприяє більш глибокому засвоєнню знань і підвищенню підготовленості до надзвичайних ситуацій.
Аналітика та прогнозування ризиків	Використання великих даних (Big Data) та штучного інтелекту (ШІ) дозволяє аналізувати інформацію про інциденти та умови праці, а також прогнозувати потенційні ризики. На основі історичних даних системи можуть передбачати можливі небезпечні ситуації та пропонувати заходи для їх запобігання. Це забезпечує перехід до проактивного управління охороною праці.
Підвищення ефективності управління охороною праці	Інтегровані цифрові системи управління охороною праці дозволяють централізовано керувати всіма аспектами безпеки праці, від моніторингу умов до обліку інцидентів та звітності. Це значно спрощує процеси управління, знижує ймовірність людських помилок і забезпечує ефективне дотримання нормативних вимог.
Індивідуальний підхід до охорони праці	Носимі пристрої (wearables), які відстежують фізичний стан працівників (наприклад, частоту серцевих скорочень, температуру тіла, рівень стресу), дозволяють забезпечити індивідуальний підхід до охорони праці. Це допомагає вчасно виявляти ознаки перевтоми, стресу чи інших загроз здоров'ю та вживати заходів для запобігання небезпекам.
Цифрова звітність та прозорість	Цифровізація спрощує створення звітів з охорони праці, роблячи цей процес автоматизованим і прозорим. Це дозволяє знизити адміністративне навантаження на персонал, а також забезпечити точність і своєчасність подання звітності.
Забезпечення відповідності нормативним вимогам	Цифрові системи допомагають забезпечити відповідність підприємства всім нормативним вимогам щодо охорони праці. Вони можуть автоматично оновлювати нормативні бази, стежити за дотриманням стандартів і попереджати про необхідність проведення певних заходів або оновлення документації.
Захист від кіберзагроз	Цифровізація також висуває нові вимоги до кібербезпеки, оскільки охорона праці стає залежною від цифрових систем. Захист інформаційних систем від кіберзагроз стає критично важливим для забезпечення безпеки працівників та безперебійної роботи підприємства.

Цифровізація створює нові можливості для підвищення ефективності охорони праці, робить цей процес більш прозорим і керованим, але також потребує належного захисту від кіберзагроз та постійного оновлення знань працівників і керівників.

Формування культури безпеки на підприємстві є важливим аспектом виробничої безпеки. Це означає, що всі працівники, незалежно від їхньої посади, повинні розуміти важливість дотримання правил безпеки і брати активну участь у створенні безпечного робочого середовища. Культура безпеки також передбачає відкритість до обговорення проблем безпеки і готовність до навчання та вдосконалення.

Культура безпеки – це загальний термін для концепції безпеки, поінформованості про безпеку та різних видів поведінки, в основному включаючи концепцію безпеки, безпеку поведінки, безпеку системи, безпеку процесу та її значення особливо помітно в енергетиці, електроенергетиці, хімічній та інших галузях промисловості. Конкретні об'єкти дослідження культури безпеки поділяються на чотири категорії:

1) культура концепції безпеки;
2) культура безпечної поведінки;
3) культура управління безпекою;
4) культура фізичного стану безпеки.

Безпека висувається з точки зору фізичних і психічних потреб людей, спрямована на людей і речі, прямо чи опосередковано пов'язана з фізичними і психічними потребами людей. Культура безпеки застосовується до високотехнологічних і високоризикових операційних підприємств, шляхом культивування цінностей безпеки та норм безпеки поведінки, визнаних працівниками, самодисципліни, самоуправління та управління командою, які створюються на підприємстві Культурна атмосфера – мета постійного покращення показників безпеки та створення довгострокового механізму безпечного виробництва. Культура безпеки полягає в процесі виживання, відтворення та розвитку людини, у всіх сферах виробництва, життя та практики, щоб забезпечити фізичну та психічну безпеку людини (включаючи здоров'я) і дозволити їй брати участь у всіх видах діяльності безпечно, комфортно та ефективно.

Культура безпеки необхідна для того, щоб запобігти, уникнути, контролювати та ліквідувати аварії та катастрофи (природні, техногенні чи природні катастрофи); створити безпечне, надійне, гармонійне та скоординоване середовище та систему безпеки для відповідних операцій; зробити людей безпечнішими. Культура безпеки має широке та вузьке значення, але з точки зору її виникнення та процесу розвитку, глибоке значення культури безпеки належить до категорії «освіти безпеки», «культивування безпеки» або «якості безпеки».

Використання засобів культури безпеки призначене лише для компенсації внутрішнього недоліку, що засоби управління безпекою не можуть повністю змінити небезпечну поведінку людей. Роль культури безпеки полягає в тому, щоб постійно підвищувати якість безпеки людей шляхом зміцнення гуманістичних факторів, таких як людські концепції, мораль, етика, ставлення, емоції та поведінка, а також за допомогою лідерства, освіти, публічності, винагород і покарань, створення атмосфери. По суті безпека є різновидом культури, важливою її частиною. Це важлива гарантія захисту та розвитку продуктивності, важливий символ соціальної цивілізації та національної всеосяжної сили; це основний критерій сучасного науково-технічного розвитку та соціального розвитку, втілення соціальної ефективності [1].

Культура безпеки розглядається у контексті гуманістичної етики, культури та освіти; це символ естетики та антропології, які є основою культивування людської природи, норм поведінки, моральних понять, цінностей і поглядів на життя. Культура безпеки була вперше висунута після аварії на Чорнобильській АЕС, щоб вирішити проблеми ядерної безпеки, тому історія розвитку культури безпеки є історією розвитку теорії причин аварії. Поява літаків під час Другої світової війни сприяла дослідженню ергономіки в галузі промислової безпеки. Люди висунули нові теорії про причини аварій: теорію перетину траєкторій і теорію аварійних зустрічей, так що в центрі уваги попередження аварій. починається з людей Починається передача на речі (обладнання).

Культура безпеки базується на принципах управління безпекою, і подальший розвиток концепцій культури безпеки більше не обмежується сферою ядерної безпеки. У сфері промислової безпеки в процесі розвитку культури безпеки усвідомлюється, що запобігання нещасним випадкам на виробництві має зміцнити побудову культури безпеки підприємства. Метод управління підприємством увійшов в епоху управління культурою підприємства від простого системного управління, тобто уніфікації операційної та управлінської поведінки підприємства із загальним характером операційної культури підприємства.

Культура безпеки є частиною загальної культури підприємства та однією з основних характеристик модернізації системи управління безпекою виробництва підприємства. Можна побачити, що традиційне управління безпекою, яке спирається виключно на адміністративні методи, не може адаптуватися до розвитку ринкової економіки індустріального суспільства Побудова культури безпеки, яка об'єднує цінність виробництва та реалізації людей, є основою для побудови підприємствами сучасного механізму управління безпекою. EESCS – це набір практичних і здійсненних

організаційних установок безпеки, поведінки в галузі безпеки та індивідуальних установок щодо безпеки та методів управління поведінкою в сфері безпеки, спрямованих на людей та їхню надійність. Культура ядерної безпеки є джерелом культури безпеки.

МАГАТЕ поділяє розвиток культури безпеки на три фази, кожна з яких має різні характеристики:

1) саморегуляції: безпека, заснована на правилах і нормах;
2) усвідомлений етап: хороші показники безпеки стають метою організації;
3) ефективність безпеки завжди можна покращити. Безпека повинна стати основною умовою для всієї роботи в компанії.

Будучи важливим способом підвищення рівня управління безпекою на підприємстві та реалізації внутрішньої безпеки підприємств, побудова культури безпеки є проектом, який приносить користь життю, здоров'ю та безпеці працівників. Підприємства та організації повинні посилити будівництво культури безпеки підприємства, просувати демонстраційний проект будівництва культури безпеки, посилити будівництво позицій культури безпеки, інноваційні форми, збагачувати зміст, формувати рушійні сили. Побудова культури безпеки – це команда та група, яка служить основою безпеки підприємства. Необхідно побудувати систему побудови культури безпеки для колективів підприємств.

Ключем до побудови культури безпеки компанії є зосередження на «будівництві», яке гарантується сильним організаційним керівництвом, упорядкованим робочим механізмом та ефективними заходами просування. Заходи захисту: відповідно до характеру та характеристик різних підрозділів, направляти підрозділи для створення відповідних моделей побудови культури безпеки, створити систему створення стандартизації виробництва безпеки, покращити систему оцінки якості навчання з безпеки; посилити інвестиції в побудову культури безпеки, рекомендувати команди з організації культури безпеки.

Мета дослідження культури безпеки полягає в тому, щоб захистити фізичну та психічну безпеку та здоров'я людей і забезпечити їм безпеку, здоров'я, комфорт та ефективну участь у всіх видах діяльності, попередження, запобігання, контроль та ліквідацію аварій і катастроф (викликані катастрофами та стихійними лихами) і ризики, створені безпечним матеріальним багатством і безпечним духовним багатством. Дослідження та розвиток культури безпеки людини спрямовані на реалізацію підтримки та захисту права людей на виживання, працю та життя шляхом встановлення концепції безпеки «орієнтованої на людей».

Концепція культури безпеки була офіційно висунута в середині та наприкінці 1980-х рр. Вперше вона була висунута Міжнародним агентством

з атомної енергії в аналізі аварії на Чорнобильській АЕС у Радянському Союзі 80 як контрзахід ядерної безпеки. З того часу, у 1986 році, НАСА Сполучених Штатів застосовувало культуру безпеки для управління аерокосмічною безпекою. Сьогодні ця концепція вже вийшла за рамки атомної промисловості та аерокосмічної промисловості та широко прийнята та використовується в усьому світі. Концепція культутри безпеки = це сукупність принципів, цінностей, норм, та поведінкових стандартів, які сприяють забезпеченню безпечних умов праці на підприємстві. Вона включає в себе настпуніц аспекти

Таблиця 9.29 – Концепція культури безпеки в контексті реалізації виробничої безпеки та безпеки праці

Психологічна установка на безпеку	Формування у співробітників розуміння важливості безпеки, відповідальності за власне здоров'я та життя, а також життя і здоров'я колег.
Системний підхід до управління безпекою	Інтеграція питань безпеки в усі аспекти діяльності підприємства, від стратегічного планування до щоденних операцій.
Навчання та інформування	Постійне навчання персоналу правилам та процедурам безпеки, підвищення їхньої обізнаності про потенційні ризики та методи їхнього попередження.
Комунікація та зворотній зв'язок	Створення каналів для відкритої комунікації щодо питань безпеки, заохочення обговорення проблем та обміну ідеями щодо їх вирішення.
Профілактика та попередження	Запровадження заходів, спрямованих на попередження небезпечних ситуацій, проведення регулярних аудитів та оцінки ризиків.
Відповідальність керівництва	Активна участь керівництва у впровадженні та підтримці культури безпеки, їхня відповідальність за створення безпечних умов праці.
Мотивація та винагорода	Розробка системи мотивації, яка заохочує працівників до дотримання правил безпеки, а також до участі у покращенні безпеки на робочому місці.
Безперервне вдосконалення	Постійний аналіз результатів, впровадження інновацій та покращення процесів, спрямованих на підвищення рівня безпеки праці.
Розвиток свідомості безпеки	Формування свідомості безпеки серед працівників є основою культури безпеки. Це включає навчання та тренінги, які допомагають працівникам усвідомлювати ризики, що супроводжують їхню діяльність, і впроваджувати ефективні заходи для їхнього зниження.
Лідерство і відповідальність керівництва	Лідери організації відіграють ключову роль у формуванні та підтримці культури безпеки. Вони мають бути прикладом відповідального ставлення до безпеки, забезпечувати прозорість у питаннях безпеки праці, а також активно залучати працівників до участі у створенні безпечних умов праці.

Закінчення таблиці 9.29

Системний підхід до управління ризиками:	Включає ідентифікацію, оцінку та управління ризиками, пов'язаними з виробничими процесами. Це може бути реалізовано через впровадження сучасних систем управління охороною праці, які забезпечують постійний моніторинг і аналіз ризиків та їхнього впливу на виробничий процес.
Підтримка і розвиток технологій безпеки	Використання сучасних технологій для моніторингу умов праці, попередження аварійних ситуацій та забезпечення безпеки на робочих місцях є важливим елементом культури безпеки. Це може включати автоматизовані системи контролю, використання персональних захисних засобів та інтеграцію інноваційних рішень для мінімізації ризиків.
Залучення працівників до процесів покращення безпеки	Формування культури безпеки неможливе без активної участі працівників. Це може бути досягнуто шляхом створення механізмів зворотного зв'язку, коли працівники можуть пропонувати свої ідеї та рішення для покращення безпеки, а також через системи винагород і визнання за ініціативи в сфері безпеки.
Психологічний клімат та мотивація	Безпека праці тісно пов'язана з психологічним кліматом в колективі. Створення атмосфери довіри та підтримки, де працівники не бояться повідомляти про проблеми або небезпечні умови, сприяє розвитку культури безпеки. Мотиваційні програми, що підкреслюють важливість безпеки і здоров'я, також відіграють ключову роль.
Контроль та оцінка результатів	Постійний контроль та оцінка ефективності заходів з безпеки є необхідними для підтримання високого рівня культури безпеки. Це включає регулярний аудит, аналіз інцидентів, а також адаптацію та вдосконалення заходів з урахуванням нових викликів та технологій.

Культура безпеки є ключовим фактором у створенні безпечного виробничого середовища, зниженні рівня травматизму та професійних захворювань, а також підвищенні ефективності роботи підприємства загалом. Концепція культури безпеки у контексті виробничої безпеки та безпеки праці охоплює системний підхід до забезпечення захисту життя і здоров'я працівників, зниження ризиків виробничих травм та професійних захворювань, а також сприяє формуванню відповідальної поведінки на робочому місці. Таким чином, культура безпеки у контексті виробничої безпеки та безпеки праці є інтегрованим підходом, що об'єднує технічні, організаційні та психологічні аспекти з метою забезпечення здорових і безпечних умов праці, зниження кількості травм та професійних захворювань, а також підвищення загальної ефективності виробничого процесу.

Культура безпеки, з точки зору великої безпеки та великої культури, є сумою концепцій, поведінки та фізичних станів безпечного виробництва та безпечного життя, створених діяльністю людини з безпеки. Культура безпеки як складова соціальної відповідальності організацій – це цінність

безпеки та кодекс поведінки, які пропагують на рівні прийняття рішень і визнають усі працівники після тривалого накопичення, безперервного узагальнення та вдосконалення в практиці виробництва безпеки. Це усвідомлення безпеки, віра в безпеку, звичка безпеки, безпека Всебічне відображення етики, традицій безпеки, норм безпеки, технологій безпеки та продуктів безпеки.

Побудова культури безпеки, яка усвідомлює цінність виробництва та цінність людей, є основним способом для підприємств подолати бар'єр безпеки поганого циклу «аварія-усунення-перевірка-повтореннявиправлення-повторна перевірка» Культура безпеки як складова соціальної відповідальності організацій виконує функцію регулювання поведінки людей, а її основними функціями є:

1) Направляюча функція: те, що підтримується і захоплюється культурою безпеки підприємства, сприйме загальні цінності через непомітний вплив, і увага працівників неминуче звернеться до змісту, який підтримується та захоплюється, і направлятиме особисті цілі працівників до цілей підприємства.

2) Функція когезії: коли члени підприємства визнають цінність корпоративної культури безпеки, вона стане своєрідним сполучною речовиною, що об'єднує її членів з усіх аспектів, утворюючи величезну доцентрову силу та згуртованість, яка є культурною силою.

3) Стимулююча функція: функція культурної влади стосується ефекту, який культурна сила може змусити членів підприємства почуватися піднесеними та заповзятливими від усього серця. Даючи повний простір людській ініціативі, творчості, ентузіазму та мудрості, вона може надихати людей.

4) Функція обмеження: культурна влада має обмежувальний і нормативний вплив на мислення та поведінку кожного члена підприємства. Обмежувальна функція культурної влади відрізняється від традиційної теорії менеджменту, яка просто підкреслює жорсткі обмеження системи. Хоча вона також містить письмові жорсткі системні обмеження, вона підкреслює неписані м'які обмеження.

5) Навчання: програма постійного вдосконалення культури безпеки допомагає державам-членам зміцнювати та підтримувати їх культуру безпеки; включає тренінги, які дозволять персоналу навчених організацій використовувати оцінки культури безпеки для покращення культури безпеки, розробки ефективних програм покращення та ініціювання ефективних та стійких організаційних змін. МАГАТЕ визначає сильну культуру безпеки як сукупність організаційних та індивідуальних характеристик і ставлень, які надають питанням захисту та безпеки найвищий пріоритет і належну увагу до їх важливості.

Щоб покращити культуру безпеки, потрібне всебічне розуміння загальної культури організації. Самооцінка культури безпеки допомагає організаціям визначити ставлення, основні переконання та припущення, що лежать в основі поведінки. Висновки дозволили організації відзначити сильні та слабкі сторони та закласти основу для розробки ефективних програм для підвищення культури безпеки.

Культура безпеки як складова соціальної відповідальності організацій формує цінності:

1) Економічна цінність. Безпека є передумовою економічного розвитку, а безпека є запорукою економічного розвитку. Зміцнення побудови культури безпеки та забезпечення безпечного виробництва може захистити та сприяти розвитку продуктивності. Співвідношення між превентивними інвестиціями та усуненням аварій, а також правило піраміди користі від безпеки показують, що «коефіцієнт витрат-виходів» запобіжних заходів вище, ніж «коефіцієнт витрат-виходів» усунення аварій, а співвідношення цих двох дорівнює 1:5. Це основний кількісний закон економіки безпеки. Якщо ми зосередимося на підкресленні культури безпеки в конкретних виробничих роботах з безпеки, то це пропорційне співвідношення буде переписано.

2) Управлінська цінність. Культура безпеки – це духовне досягнення, створене людьми в довгостроковому виробництві та житті. Вона може змусити керівників підприємств і працівників інтегруватися в середовище колективних емоцій безпеки, створити самообмежувальний механізм контролю безпеки та дозволити підприємствам використовувати кожен Інше. Нещільна група, утворена суспільством, перетворюється на колектив зі спільними цінностями, спільними прагненнями та згуртованістю. Для підприємств це не тільки сучасна ідея управління безпекою, але й ефективний метод управління безпекою, основа для вдосконалення системи управління безпекою, підвищення якості поведінки персоналу, побудови сучасної моделі управління безпекою. Побудова культури безпеки є не тільки потребою сучасного промислового соціального менеджменту та управління підприємством, але й потребою здорового розвитку суспільства та підприємств.

3) Соціальна цінність. Для суспільства безпека є відображенням якості життя людини. Культура безпеки наголошує на вивченні світу за допомогою абсолютно нових методів мислення та нових концепцій технологій безпеки, що пройшли протягом століть, наукового та об'єктивного розуміння життя, цінування життя та створення світлого майбутнього безпеки людей, здоров'я, комфорту, довголіття та соціальної стабільності та розвитку.

Відображенням культура безпеки як складової соціальної відповідальності організацій на філософському рівні є епістемологія та методологія

людей щодо діяльності з безпеки, фундаментальні погляди людей на те, що таке безпека та як її реалізувати. Безсумнівно, це втілює в собі душу культури безпеки та є її ключовими елементами.

По-перше, культура безпека культивує «відносність стану». Це розглядається з точки зору відносного і абсолютного характеру розвитку речей. Суть осягнення безпечного виробництва полягає в подовженні відносності безпеки та зниженні абсолютності аварійності. Деякі компанії можуть досягти довгострокових рекордів, тоді як інші мають часті нещасні випадки.

По-друге, культура безпеки включає «теорії культурної сутності» безпеки. Загалом культура безпеки включає чотири аспекти: 1) матеріальна культура. Наприклад, при виборі технології обладнання це не стільки порівняння технічних переваг і недоліків, скільки вибір методів виробництва і культурних стилів; 2) культура поведінки; 3) інституційна культура. Система є сполучною ланкою між технологіями та працівниками, і до цієї категорії відносяться безпечні процедури та системи фінансово-економічної безпеки; 4) духовна культура.

По-третє, безпека є результатом не стільки ряду матеріальних засобів, скільки культурних впливів. Культура безпеки поширена в різних елементах виробництва підприємства та об'єднує ці елементи для формування сили безпеки. По суті, культура безпеки як складова соціальної відповідальності організацій – це культура, яка захищає здоров'я людей, цінує життя людей і усвідомлює цінність людей, її важливою особливістю є те, що він втілює сильну гуманістичну турботу та ціннісну орієнтацію.

9.6 ЦИВІЛЬНА БЕЗПЕКА

Інтеграція цифрових технологій у систему цивільної безпеки з урахуванням нових викликів і можливостей має велику актуальність у сучасному світі, так як відбуваються щвидкі технологічні зміни, зростаючі загрози, підвищення ефективності реагування, необхідність оптимізації ресурсів. До актуальних причин аналізу цивільної безпеки у сучасному небезпечному світі слід віднести наступні:

1) Швидкий темп технологічного розвитку створює нові можливості для підвищення ефективності та ефективності систем цивільної безпеки. Розуміння цих технологій та їхній інтеграції стає критично важливим.

2) Сучасні загрози, такі як кібератаки, терористичні акти, екологічні катастрофи та інші, вимагають нових підходів до забезпечення цивільної безпеки. Використання цифрових технологій може допомогти в ефективному протистоянні цим загрозам.

3) Інтеграція цифрових технологій у систему цивільної безпеки може значно підвищити швидкість та ефективність реагування на надзвичайні ситуації та кризові події.

4) Використання цифрових технологій може допомогти оптимізувати використання ресурсів у сфері цивільної безпеки, забезпечуючи ефективнішу роботу за менші витрати.

5) Світ постійно змінюється, і системи цивільної безпеки повинні постійно адаптуватися до нових викликів та можливостей. Розуміння цифрових технологій допоможе забезпечити, що ці системи залишаються актуальними та ефективними.

Цивільна оборона у контексті нових викликів та можливостей означає адаптацію систем цивільного захисту до сучасних реалій, включаючи нові загрози, технологічні зміни та економічні виклики. Цивільна безпека передбачає застосування інноваційних підходів, в тому числі цифрових технологій, для підвищення ефективності та адаптивності систем цивільного захисту до сучасних умов.

Таблиця 9.30 – Застосування сучасних підходів цивільного захисту

Сучасні підходи	Зміст та характеристика
Врахування нових видів загроз	Врахування нових видів загроз, таких як кібератаки, гібридна війна, терористичні атаки, біологічні або хімічні загрози, і розробка відповідних стратегій протидії.
Застосування цифрових технологій	Застосування цифрових технологій, таких як штучний інтелект, аналіз даних, блокчейн, віртуальна реальність для підвищення швидкості та ефективності реагування в надзвичайних ситуаціях
Розробка механізмів забезпечення стійкості	Розробка механізмів забезпечення стійкості та відновлюваності інфраструктури в разі надзвичайних ситуацій, включаючи технології для прогнозування, попередження та відновлення після кризових подій.
Підвищення свідомості та готовності населення:	Здійснення програм з підвищення свідомості та готовності населення до можливих загроз і дій в надзвичайних ситуаціях, використовуючи цифрові засоби комунікації та освітні ресурси.
Обмін досвідом між країнами у сфері цивільного захисту	Зміцнення співпраці та обміну досвідом між країнами у сфері цивільного захисту з метою ефективного вирішення спільних викликів та загроз.

Аналіз сучасного стану системи цивільної оборони та готовності до впровадження цифрових технологій може включати наступні аспекти:

1) Оцінка існуючих методів та технологій, які використовуються в системі цивільної оборони, що може включати системи моніторингу, комунікації, реагування на надзвичайні ситуації та інші.

2) Аналіз наявної інфраструктури та ресурсів, які можуть бути використані для впровадження цифрових технологій, що включає доступ до мережі Інтернет, обладнання, кваліфікацію персоналу та інше.

3) Захист від кіберзагроз, в основі якого оцінка рівня захисту системи цивільної оборони від кіберзагроз, що може включати оцінку існуючих заходів з кібербезпеки, виявлення слабких місць та розробку стратегій їх усунення.

4) Ступінь готовності персоналу та керівництва, в основі якого аналіз готовності персоналу та керівництва до впровадження цифрових технологій. Це включає оцінку рівня технічної компетентності, готовності до змін та підтримки нововведень.

5) Розгляд правових та етичних аспектів використання цифрових технологій у системі цивільної оборони. Це може включати питання конфіденційності даних, захисту приватності громадян, а також дотримання відповідних законодавчих норм та міжнародних стандартів.

6) Ідентифікація потенційних викликів та можливостей, в основаі яких оцінка потенційних викликів, які можуть виникнути у майбутньому в контексті цивільної оборони, а також визначення можливостей, які можуть бути використані для вдосконалення системи за допомогою цифрових технологій. Це може включати такі фактори, як зміни клімату, терористичні загрози, масові протести тощо.

7) Оцінка технічних можливостей та обмежень, в основі яких аналіз технічних можливостей та обмежень впровадження цифрових технологій у систему цивільної оборони. Це включає оцінку доступності та сумісності існуючих систем з новими технологіями, потенційні технічні складнощі та інші аспекти.

8) Визначення пріоритетів та стратегії розвитку, в основі яких встановлення пріоритетів у впровадженні цифрових технологій на основі аналізу потреб, викликів та можливостей; розробка стратегії розвитку, що враховує короткострокові та довгострокові цілі, а також ресурсні обмеження.

9) Залучення зацікавлених сторін та партнерство, що включає встановлення партнерств та співпраці з іншими установами, компаніями та громадськими організаціями для спільного розвитку та впровадження цифрових ініціатив у сфері цивільної оборони.

10) Створення механізмів моніторингу та оцінки ефективності, в основі яких розробка системи моніторингу та оцінки ефективності впроваджених цифрових технологій у системі цивільної оборони.

Цивільна безпека також включає співпрацю з іншими державами та міжнародними організаціями для обміну досвідом, спільної координації дій у випадку великих катастроф. Важливим компонентом є створення законодавчої бази, що регламентує діяльність у сфері цивільної безпеки, визначає обов'язки органів влади, підприємств та громадян.

Таблиця 9.31 – Основні компоненти цивільної безпеки

Основні компоненети	Зміст та характеристика
1	2
Захист населення від надзвичайних ситуацій природного характеру	Природні катастрофи: землетруси, повені, урагани, пожежі, зсуви та інші природні явища, які можуть становити загрозу для життя і здоров'я населення. Метеорологічні ризики: захист населення від екстремальних погодних умов, таких як сильні морози, спека, штормові вітри.
Захист населення від техногенних катастроф	Промислові аварії: вибухи, пожежі, викиди небезпечних речовин на підприємствах, витоки нафтопродуктів. Транспортні аварії: аварії на автомобільному, залізничному, авіаційному та морському транспорті. Аварії на об'єктах життєзабезпечення: пошкодження об'єктів інфраструктури, таких як електростанції, водопостачальні мережі, газопроводи.
Готовність до надзвичайних ситуацій та реагування на них	Планування та підготовка: розробка планів дій на випадок надзвичайних ситуацій, навчання та тренування населення і служб цивільного захисту. Системи раннього попередження: впровадження систем моніторингу та оповіщення для виявлення загроз та інформування населення. Евакуація та притулки: організація евакуації населення з небезпечних зон, створення і підтримка укриттів.
Охорона громадського порядку та безпека в надзвичайних ситуаціях	Підтримка порядку: запобігання масовим заворушенням, забезпечення громадського порядку під час надзвичайних ситуацій. Контроль за доступом до небезпечних зон: організація контрольованого доступу до зон, де існує підвищений ризик для життя.
Медичне забезпечення	Екстрена медична допомога: організація надання першої медичної допомоги постраждалим, евакуація поранених, підтримка лікарень і медичних закладів. Епідеміологічна безпека: попередження і контроль за розповсюдженням інфекційних захворювань, особливо під час надзвичайних ситуацій.
Інформаційна безпека та комунікації	Інформування населення: надання достовірної та оперативної інформації про ситуацію та дії, що вживаються для забезпечення безпеки. Захист інформаційних систем: забезпечення захисту комунікаційних мереж, що використовуються для управління кризовими ситуаціями.
Психологічна підтримка населення	Психологічна допомога: організація служб психологічної підтримки для населення, яке постраждало від надзвичайних ситуацій. Реабілітація постраждалих: заходи щодо відновлення психічного здоров'я осіб, які зазнали впливу надзвичайних ситуацій.

Продовження таблиці 9.31

1	2
Забезпечення економічної стабільності під час кризи	Підтримка економічних систем: заходи, спрямовані на збереження економічної активності, забезпечення роботи критичної інфраструктури і основних галузей економіки. Допомога постраждалим: надання фінансової допомоги постраждалим громадам, відшкодування збитків, відновлення інфраструктури.
Забезпечення соціальної безпеки	Надання підтримки найбільш вразливим категоріям населення під час і після надзвичайних ситуацій. Це включає виплату соціальних допомог, забезпечення житлом, продовольством, медичними послугами та іншими життєво необхідними ресурсами.
Підтримка громадського порядку	Організація громадської допомоги та волонтерського руху для підтримки населення під час кризових ситуацій. Це включає мобілізацію ресурсів, координацію дій громадських організацій, навчання волонтерів.
Захист від кібератак	Охорона інформаційних систем та мереж, що забезпечують життєдіяльність суспільства, від кібератак, зловмисного програмного забезпечення, зламів. Забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів.
Управління інформацією під час криз	Координація інформаційних потоків для забезпечення громадян точною та своєчасною інформацією під час надзвичайних ситуацій. Це включає створення центрів кризового інформування, використання засобів масової інформації, соціальних мереж для інформування громадян про загрози та дії з їхньої сторони.
Психологічна підтримка у кризових ситуаціях	Організація психологічної допомоги для постраждалих осіб, що пережили катастрофи, аварії, соціальні заворушення або інші кризові події. Це може включати надання консультацій, проведення групових терапій, реабілітаційних програм.
Психологічна підготовка населення	Розробка і проведення програм, спрямованих на підвищення психологічної стійкості населення перед можливими кризовими ситуаціями. Це включає навчання навичок самоконтролю, управління стресом, прийняття рішень в умовах невизначеності.
Розробка законодавчої бази	Створення та підтримка законодавчих і нормативних актів, що регулюють питання цивільної безпеки. Це включає закони, що визначають права та обов'язки громадян, підприємств і державних органів у разі надзвичайних ситуацій. Організація моніторингу та контролю за виконанням законодавства у сфері цивільної безпеки, а також притягнення до відповідальності осіб, які порушують ці вимоги.
Співпраця з міжнародними організаціями	Забезпечення участі в міжнародних програмах цивільної безпеки, що спрямовані на попередження глобальних загроз, таких як тероризм, зміни клімату, великі природні катастрофи. Координація дій з іншими країнами та міжнародними організаціями для оперативного реагування на кризи.

Закінчення таблиці 9.31

1	2
Надання гуманітарної допомоги	Організація та участь у міжнародних гуманітарних операціях для надання допомоги країнам, що постраждали від природних або техногенних катастроф. Це може включати постачання медикаментів, продуктів харчування, засобів гігієни, а також надання експертної допомоги в ліквідації наслідків катастроф.

Ці компоненти утворюють комплексний підхід до захисту громадян. Цивільна безпека, завдяки своїм численним компонентам, забезпечує захист населення і суспільства в цілому від різноманітних загроз, сприяючи збереженню життєдіяльності, стабільності та добробуту громадян у надзвичайних ситуаціях.

Безпека праці є важливим аспектом будь-якого суспільства, оскільки забезпечення безпечних умов праці має прямий вплив на загальну цивільну безпеку. Безпека праці включає в себе комплекс заходів, спрямованих на захист працівників від виробничих ризиків, що можуть призвести до травм, захворювань або інших небажаних наслідків. У свою чергу, цивільна безпека залежить від ефективної реалізації цих заходів на рівні підприємств, організацій та держави загалом. Безпека праці є важливою складовою цивільної безпеки, оскільки її забезпечення сприяє стабільності суспільства, збереженню здоров'я та життя громадян, а також запобіганню техногенних катастроф.

Таблиця 9.32 – Основні аспекти взаємозв'язку між безпекою праці та цивільною безпекою

Основні аспекти	**Зміст та характеристика**
1	2
Захист працівників	Основне завдання безпеки праці – забезпечити захист працівників від виробничих ризиків, які можуть мати негативний вплив на їх здоров'я і життя. Це сприяє збереженню трудових ресурсів, зменшенню витрат на лікування та соціальне забезпечення постраждалих.
Стабільність економіки	Безпека праці сприяє підвищенню продуктивності праці та зменшенню кількості нещасних випадків на виробництві, що, в свою чергу, позитивно впливає на економічну стабільність. Стабільна економіка є основою для забезпечення цивільної безпеки, оскільки зменшує ризики соціальних конфліктів та забезпечує стале функціонування держави. Небезпечні умови праці можуть призводити до підвищеного рівня травматизму, професійних захворювань та загальної незадоволеності працівників, що створює ризики соціальних конфліктів.

Продовження таблиці 9.32

1	2
Стабільність економіки (продовж)	У свою чергу, високий рівень безпеки праці сприяє зменшенню соціальної напруги, підвищенню довіри працівників до роботодавців і держави, що є важливим чинником стабільності в суспільстві.
Профілактика техногенних катастроф	Дотримання правил безпеки на виробництві дозволяє знизити ризик техногенних катастроф, які можуть призвести до значних втрат як серед працівників, так і серед населення. Такі катастрофи можуть мати серйозні наслідки для цивільної безпеки, включаючи порушення життєдіяльності суспільства, економічні збитки та екологічні проблеми.
Роль держави у забезпеченні безпеки праці	Держава відіграє ключову роль у регулюванні питань безпеки праці шляхом встановлення стандартів, нагляду за їх виконанням та забезпечення прав працівників. Ефективна державна політика у цій сфері сприяє створенню безпечних умов праці та знижує рівень професійних ризиків, що є важливою складовою цивільної безпеки.
Освітня та інформаційна робота	Підвищення рівня обізнаності працівників та роботодавців про важливість дотримання правил безпеки є ключовим елементом у запобіганні виробничим травмам і катастрофам. Інформаційні кампанії, навчальні програми та тренінги сприяють формуванню культури безпеки, що є основою для забезпечення як безпеки праці, так і загальної цивільної безпеки.
Взаємозв'язок з екологічною безпекою	Забезпечення безпечних умов праці має безпосередній вплив на екологічну безпеку. Виробництва, що не дотримуються стандартів безпеки, можуть стати джерелами екологічних загроз, включаючи забруднення повітря, води та ґрунтів, що, в свою чергу, створюють ризики для здоров'я населення і стабільності екосистем. Тому інтеграція безпеки праці з екологічною політикою є ключовим завданням для забезпечення цивільної безпеки в цілому.
Технологічні інновації та їх роль у підвищенні безпеки праці	Сучасні технологічні досягнення значно підвищують рівень безпеки праці. Використання автоматизації, роботизації та штучного інтелекту дозволяє знизити ризик травматизму, зменшити вплив людського фактора і підвищити ефективність виробничих процесів. Це, в свою чергу, сприяє зниженню рівня виробничих інцидентів, що підвищує загальний рівень цивільної безпеки.
Міжнародні стандарти та обмін досвідом	Забезпечення безпеки праці вимагає відповідності міжнародним стандартам, таким як ISO 45001, а також активного обміну досвідом між країнами. Інтеграція міжнародних стандартів сприяє підвищенню рівня безпеки національних виробництв і зменшує кількість нещасних випадків. Міжнародна співпраця у сфері безпеки праці також є важливим елементом глобальної цивільної безпеки.
Правове забезпечення та контроль за дотриманням стандартів	Правове регулювання є фундаментальним елементом забезпечення безпеки праці. Держави повинні мати ефективні закони, які регулюють стандарти безпеки, а також механізми контролю за їх дотриманням. Регулярні інспекції, штрафи за порушення та програми мотивації для підприємств, що дотримуються високих стандартів, є важливими інструментами для підтримки високого рівня безпеки праці.

Закінчення таблиці 9.32

1	2
Психологічний аспект безпеки праці	Не менш важливим є психологічний аспект безпеки праці. Роботодавці повинні піклуватися не лише про фізичну безпеку працівників, але й про їхній психологічний стан. Стрес, перевантаження та незадоволеність умовами праці можуть призвести до зниження ефективності праці та підвищення рівня аварійності. Створення позитивного робочого середовища, де працівники почуваються захищеними та оціненими, сприяє загальній безпеці та стабільності.
Соціальна відповідальність бізнесу	Відповідальний бізнес, який приділяє увагу безпеці праці, не лише зменшує ризики для своїх працівників, але й сприяє зміцненню соціальної структури суспільства. Корпоративна соціальна відповідальність у сфері безпеки праці включає активне інвестування в захисні заходи, навчання працівників, а також участь у суспільних ініціативах, що спрямовані на підвищення загального рівня безпеки.

Таким чином, безпека праці є базовим елементом, на якому будується цивільна безпека. Вона впливає на економічну стабільність, соціальний мир, екологічну безпеку, технологічний розвиток і загальний добробут суспільства. Забезпечення безпечних умов праці має бути пріоритетом для держав, підприємств і громадян, оскільки це ключ до сталого розвитку та захисту суспільства від внутрішніх і зовнішніх загроз. Безпека праці є важливою складовою цивільної безпеки, оскільки її забезпечення сприяє стабільності суспільства, збереженню здоров'я та життя громадян, а також запобіганню техногенних катастроф.

Важливим для нас є досвід зарубіжних країн у сфері цивільної безпеки є багатогранним і відображає різноманітність підходів до захисту населення від різних загроз, включаючи природні катастрофи, терористичні акти, технологічні аварії тощо.

Завдяки цим заходам країни підтримують високий рівень готовності свого цивільного населення до різних загроз, що дозволяє мінімізувати втрати та ефективно реагувати на надзвичайні ситуації. Кожна з цих країн має власний підхід до цивільної безпеки, враховуючи географічні, політичні та соціальні особливості, але всі вони мають спільну мету. Ці приклади показують, як різні країни адаптують свої системи цивільної безпеки до власних умов, зокрема до географічних, політичних та соціальних особливостей. Різноманітність підходів свідчить про необхідність комплексного та гнучкого підходу до цивільної безпеки, яка в високорозвинутих країнах дуже витребувана.

Таблиця 9.33 – Зарубіжний досвід забезпечення цивільної безпеки

Країна	Орган	Програма
1	2	3
США	Федеральне агентство з надзвичайних ситуацій (FEMA): FEMA є ключовим органом, відповідальним за координацію дій у разі надзвичайних ситуацій у США. Агентство забезпечує підготовку, реагування та відновлення після надзвичайних ситуацій. У США широко розвинені програми підготовки громадян до надзвичайних ситуацій, такі як CERT (Community Emergency Response Team), де звичайні громадяни навчаються базовим навичкам першої допомоги та реагування на катастрофи.	Програма захисту критичної інфраструктури: Ця програма спрямована на захист критичних об'єктів, таких як енергетичні системи, транспортні мережі та водопостачання, від різних загроз, включаючи кібернетичні атаки.
Німеччина	Федеральне відомство цивільного захисту та допомоги в надзвичайних ситуаціях (BBK): Німеччина має добре розвинену систему цивільного захисту, яка включає як федеральний, так і регіональний рівні. BBK координує діяльність з підготовки до надзвичайних ситуацій, зокрема забезпечення попередження і реагування на природні катастрофи, техногенні аварії та терористичні загрози.	У Німеччині активно використовується система попередження населення, яка включає як традиційні методи (сирени, радіо), так і сучасні технології (мобільні додатки, SMS).
Японія	Національне агентство з управління катастрофами (NDMA): Японія має одну з найсучасніших систем управління катастрофами у світі. Через часті землетруси та цунамі країна розробила високорозвинені методи попередження та евакуації населення. Велика увага приділяється освіті громадян, починаючи з дитячого віку.	В Японії активно використовуються технології для моніторингу та передбачення природних катастроф, таких як системи раннього попередження про землетруси та цунамі.
Швеція	Шведське агентство цивільних надзвичайних ситуацій (MSB): MSB відповідає за координацію зусиль з підготовки, реагування та відновлення після надзвичайних ситуацій. Швеція відома своїм підходом до «цілісної оборони», де цивільна безпека інтегрується з військовими і неурядовими організаціями для забезпечення безпеки населення.	Навчання громадян: Швеція активно залучає громадян до підготовки до надзвичайних ситуацій через масові кампанії з інформування, включаючи розповсюдження буклетів з інструкціями про те, як діяти в різних кризових ситуаціях.

Продовження таблиці 9.33

1	2	3
Ізраїль	Національна система цивільної оборони (Home Front Command): Ізраїль має особливу систему цивільної оборони через постійні загрози терористичних атак та ракетних ударів. Важлива роль відводиться побудові укриттів, навчанням з евакуації та першої допомоги. Кожен громадянин має доступ до інструкцій, як діяти під час обстрілу, і де знаходяться найближчі укриття.	Ізраїль має розвинену систему раннього попередження про ракетні атаки, що включає сирени, смс-повідомлення, мобільні додатки та інші засоби інформування громадян про наближення загрози. Це дозволяє жителям швидко знайти укриття. Мобільний додаток "Home Front Command" надає інформацію про укриття, дії під час надзвичайних ситуацій, а також дозволяє отримувати сповіщення про загрози в реальному часі.
Франція	Генеральний директорат цивільного захисту та управління кризовими ситуаціями (DGSCGC): Цей орган відповідає за координацію дій у разі надзвичайних ситуацій у Франції. DGSCGC забезпечує підготовку та навчання громадян, співпрацює з іншими державними та місцевими органами для забезпечення ефективного реагування на надзвичайні ситуації.	Система Vigipirate: Це національний план боротьби з тероризмом, що включає різні рівні готовності та заходів для захисту населення. План постійно оновлюється та адаптується до сучасних загроз.
Велика Британія	Національне агентство з надзвичайних ситуацій (NHS England's Emergency Preparedness, Resilience and Response – EPRR): Велика Британія має комплексну систему реагування на надзвичайні ситуації, що включає медичні служби, поліцію, пожежні служби та місцеві ради. Одним з ключових аспектів є готовність медичних установ до будь-яких надзвичайних ситуацій, включаючи пандемії та терористичні атаки.	Система раннього попередження (UK Alerting System): Ця система дозволяє швидко інформувати населення про надзвичайні ситуації через мобільні додатки та інші канали зв'язку.
Австралія	Агентство з надзвичайних ситуацій (Emergency Management Australia – EMA): EMA координує національні зусилля щодо реагування на природні катастрофи, такі як лісові пожежі, повені та циклони. Особлива увага приділяється співпраці з місцевими громадами та підготовці їх до можливих загроз.	Національна стратегія щодо лісових пожеж: Австралія розробила ефективну систему попередження та боротьби з лісовими пожежами, враховуючи часті пожежі на континенті. Вона включає моніторинг погоди, підготовку населення та координацію зусиль між різними органами.

Закінчення таблиці 9.33

1	2	3
Канада	Публічна безпека Канади (Public Safety Canada): Це федеральне відомство відповідає за забезпечення безпеки громадян від різних загроз, включаючи тероризм, природні катастрофи та технологічні аварії. Важливим елементом є тісна співпраця з провінційними та місцевими органами влади.	Стратегія щодо надзвичайних ситуацій (Emergency Management Strategy for Canada): Вона включає в себе чотири ключові елементи: запобігання, готовність, реагування та відновлення. Особлива увага приділяється зміцненню стійкості громад до надзвичайних ситуацій.
Івденна Корея	Національна агенція з управління надзвичайними ситуаціями (NEMA): Південна Корея, як країна з високим рівнем техногенних та природних ризиків, має розвинену систему управління надзвичайними ситуаціями. NEMA відповідає за координацію дій у разі землетрусів, повеней, тайфунів та інших природних катастроф.	Система попередження населення: Включає використання різних каналів зв'язку, таких як мобільні додатки та телевізійні трансляції, для швидкого інформування населення про надзвичайні ситуації.
Норвегія	. Норвезька дирекція цивільного захисту (DSB): DSB відповідає за підготовку та координацію зусиль у разі надзвичайних ситуацій, включаючи природні катастрофи, техногенні аварії та терористичні загрози. Особлива увага приділяється підготовці населення до екстремальних погодних умов, враховуючи географічні особливості країни.	Навчальні програми для громадян: Норвегія активно навчає громадян, особливо в сільських регіонах, базовим навичкам виживання та дій у надзвичайних ситуаціях, таких як евакуація під час лавин або повеней.
Нова Зеландія	Національне агентство з управління надзвичайними ситуаціями (NEMA): Нова Зеландія стикається з різними природними катастрофами, такими як землетруси, цунамі та вулканічні виверження. NEMA відповідає за координацію зусиль національних та місцевих органів для захисту населення.	Програма "Get Ready": Це національна кампанія, спрямована на підготовку громадян до надзвичайних ситуацій. Вона включає в себе інформування населення про ризики та заходи, які потрібно вживати до, під час та після катастрофи.

Ізраїль постійно впроваджує інноваційні підходи в сфері цивільної безпеки для підвищення ефективності захисту населення від загроз, використовуючи цифрові технології для раннього попередження. Мобільний додаток Home Front Command – це інтерактивний додаток, який дозволяє користувачам отримувати миттєві сповіщення про надзвичайні ситуації, знаходити найближчі укриття, а також надає інструкції щодо дій у випадку різних загроз, таких як ракетні обстріли, землетруси або хімічні атаки.

Додаток використовує геолокацію для надання індивідуальних попереджень в реальному часі. В Ізраїлі розроблено систему автоматичного попередження про ракетні обстріли, яка надсилає сповіщення на мобільні пристрої, а також активує сирени в регіонах, що піддаються загрозі.

Іншим напрямом є використання штучного інтелекту (ШІ), зокрема аналіз даних для прогнозування загроз: використання ШІ для аналізу великої кількості даних, отриманих з різних джерел, включаючи соціальні мережі, супутникові знімки та розвідувальну інформацію, дозволяє прогнозувати ймовірність різних загроз, таких як терористичні атаки або природні катастрофи. Ізраїль активно впроваджує ШІ у системи автоматизованого управління кризовими ситуаціями, що дозволяє швидко реагувати на загрози без втручання людини. Ізраїльські вчені та інженери розробляють нові види матеріалів, що підвищують міцність та стійкість укриттів до вибухів та інших видів руйнувань. Ці матеріали використовуються для будівництва нових укриттів та модернізації старих.

Смарт-укриття нового покоління оснащені сучасними технологіями, такими як системи очищення повітря, автономне електропостачання, доступ до інтернету та зв'язку. Це дозволяє людям перебувати в укриттях тривалий час з мінімальним дискомфортом. В Ізраїлі розробляються мобільні системи, що дозволяють швидко розгортати гуманітарну допомогу, включаючи медичну допомогу, воду, продукти харчування та інші необхідні ресурси в зонах надзвичайних ситуацій. Використання дронів для доставки медикаментів і проведення рятувальних операцій в умовах, коли доступ до зони лиха обмежений або небезпечний.

Ізраїль активно інвестує в кібербезпеку для захисту критичної інфраструктури, такої як енергетичні мережі, водопостачання, транспортні системи та комунікації. Використовуються передові системи моніторингу, які виявляють і запобігають кібератакам у реальному часі. Ізраїль розвиває спеціалізовані навчальні програми для підготовки фахівців у сфері кібербезпеки, які працюють у державних і приватних структурах. Ізраїль проводить широкомасштабні кампанії для підвищення обізнаності населення про те, як діяти в різних надзвичайних ситуаціях, включає використання соціальних мереж, відео, буклетів, а також проведення публічних заходів і тренінгів. Школи і молодіжні організації активно залучають дітей до програм підготовки, що включають симуляції надзвичайних ситуацій, навички виживання та першої допомоги. Ці інноваційні підходи дозволяють Ізраїлю підтримувати високий рівень готовності до надзвичайних ситуацій та ефективно захищати своє населення від різноманітних загроз.

Використання систем цивільної безпеки має важливе теоретичне і практичне значення, що відображається у різних аспектах суспільного

життя, державного управління та міжнародних відносин. Цивільна безпека є невід'ємною частиною концепції національної безпеки, яка включає захист населення від внутрішніх і зовнішніх загроз. Вона визначає механізми, через які держави забезпечують стійкість своїх соціальних, економічних і політичних систем перед обличчям надзвичайних ситуацій. Вивчення цивільної безпеки сприяє розвитку нових концепцій, моделей та підходів до управління кризовими ситуаціями. Це включає аналіз ризиків, розробку стратегій попередження, готовності та реагування на надзвичайні ситуації.

Системи цивільної безпеки теоретично обґрунтовують поняття соціальної стабільності та стійкості, включаючи здатність суспільства адаптуватися до загроз і відновлюватися після них. Вони розглядають, як соціальні інститути, такі як сім'я, школа, робоче місце, можуть бути залучені до забезпечення безпеки. Теоретичне вивчення цивільної безпеки включає дослідження психологічних і соціальних аспектів поведінки людей під час криз, що допомагає розробляти більш ефективні стратегії комунікації та управління.

Цивільна безпека тісно пов'язана з міжнародним правом, зокрема з нормами, що регулюють захист цивільного населення під час збройних конфліктів, катастроф і терористичних актів. Це також включає питання гуманітарної безпеки та захисту прав людини. Теоретичне вивчення цивільної безпеки сприяє формуванню міжнародних стандартів та рекомендацій, що регулюють діяльність держав у сфері захисту цивільного населення.

Системи цивільної безпеки дозволяють державам ефективно управляти кризами, попереджувати загрози та знижувати їхні наслідки. Це включає створення систем раннього попередження, розвиток інфраструктури для реагування на надзвичайні ситуації, а також підготовку населення до можливих загроз. Практичні результати досліджень у сфері цивільної безпеки допомагають удосконалювати практики реагування на надзвичайні ситуації, зокрема через проведення тренувань, симуляцій і реальних операцій з ліквідації наслідків катастроф. Цивільна безпека сприяє захисту критичної інфраструктури, такої як електромережі, водопостачання, транспортні системи, медичні установи та комунікації. Це важливо для забезпечення безперебійного функціонування суспільства навіть під час кризових ситуацій. Практичні аспекти включають розробку та впровадження планів відновлення після катастроф, що дозволяє швидко повернутися до нормального життя та мінімізувати економічні втрати.

Цивільна безпека включає заходи з підвищення обізнаності населення про ризики та способи їх уникнення. Це забезпечує мобілізацію населення та підвищення його готовності до реагування на надзвичайні ситуації.

Проведення освітніх програм і тренінгів з питань цивільної безпеки має практичне значення для формування стійких громад, здатних самостійно діяти в умовах загроз. Цивільна безпека є важливим аспектом міжнародної співпраці, що включає обмін досвідом, знаннями та технологіями між країнами для покращення готовності та реагування на глобальні загрози, такі як тероризм, природні катастрофи та пандемії. Практична реалізація включає участь у міжнародних гуманітарних місіях та операціях з ліквідації наслідків катастроф, що підвищує глобальну стійкість до криз. Цифровізація стала невід'ємною частиною сучасного суспільства, впливаючи на всі аспекти життя, включаючи цивільну безпеку. Цифрові технології можуть як зміцнити, так і послабити безпеку громадян в умовах їх впровадження. Цифровізація відкриває великі можливості для покращення цивільної безпеки, але водночас вимагає адаптації до нових викликів. Важливо балансувати між впровадженням технологій і захистом прав громадян, забезпечуючи безпечне та інклюзивне цифрове середовище для всіх. Основні аспекти впливу цифровізації на цивільну безпеку: 1) Відеокамери з функцією розпізнавання облич, системи відстеження та аналітики великих даних допомагають правоохоронним органам швидко реагувати на інциденти та попереджати злочини. 2) Мобільні додатки та інші засоби зв'язку дозволяють оперативно інформувати населення про надзвичайні ситуації, зокрема про природні катастрофи чи терористичні загрози. 3) Інтеграція цифрових технологій в інфраструктуру міст дозволяє ефективніше керувати транспортними потоками, знижуючи ризик аварій, та забезпечувати безпеку житлових районів. 4) Зростання числа кіберзлочинів, таких як хакерські атаки, крадіжка особистих даних, фішинг та інші види шахрайства, ставить під загрозу приватність та безпеку громадян. 5) Нерівний доступ до цифрових технологій може створювати соціальні бар'єри та виключати окремі групи населення з безпечного цифрового середовища. 6) Зростання використання цифрових технологій призводить до значних викликів щодо захисту персональних даних та конфіденційності. Цивільна безпека в умовах цифровізації – це комплекс заходів та стратегій, спрямованих на захист життя, здоров'я, прав і свобод громадян в умовах активного впровадження цифрових технологій у всі сфери суспільного життя. Ця концепція охоплює як переваги, так і ризики, пов'язані з цифровізацією, та включає адаптацію традиційних методів забезпечення безпеки до нових умов, створених цифровими інноваціями.

Основні компоненти цивільної безпеки в умовах цифровізації: 1) Інформаційна безпека,що включає захист інформаційних систем від несанкціонованого доступу, кібератак, крадіжки даних та інших кіберзагроз. Це включає в себе розробку законодавчих норм, технічних рішень

та освітніх програм для підвищення обізнаності населення про кібербезпеку. 2) Захист персональних даних, в основі якої забезпечення конфіденційності та недоторканності особистих даних громадян. Важливою складовою є дотримання законодавства щодо захисту даних і розробка технологій для їх безпечного зберігання та обробки. 3) Системи моніторингу та сповіщення, в основі яких використання цифрових технологій для моніторингу громадських місць, управління транспортними потоками, попередження про надзвичайні ситуації та забезпечення оперативного реагування на інциденти. 4) Розумні міста, що включають інтеграцію інформаційно-комунікаційних технологій в інфраструктуру міст для підвищення якості життя, безпеки та ефективності управління міськими ресурсами. Це включає в себе системи відеоспостереження, інтелектуальні транспортні системи та платформи для обміну інформацією. 5) Соціальна інклюзія, в основі якої забезпечення рівного доступу до цифрових технологій для всіх груп населення, зокрема для вразливих верств, з метою запобігання цифровому розриву та забезпечення безпеки і добробуту кожного громадянина.

Цивільна безпека є важливим аспектом сталого розвитку, оскільки вона забезпечує захист населення та інфраструктури від різноманітних загроз. Це включає як природні катастрофи, так і антропогенні загрози, такі як техногенні аварії, терористичні атаки та соціальні конфлікти. Цивільна безпека сприяє захисту життя і здоров'я людей, що є основою для будь-якої стратегії сталого розвитку. Забезпечення медичної допомоги, аварійно-рятувальних служб та інших механізмів реагування на надзвичайні ситуації дозволяє мінімізувати наслідки катастроф. Безпека інфраструктури є критично важливою для сталого розвитку. Це включає захист енергетичних систем, водопостачання, транспортних мереж та комунікаційних систем від різних загроз. Стійка інфраструктура забезпечує безперервність економічних і соціальних процесів. Цивільна безпека підтримує економічну стабільність, запобігаючи великим втратам, що можуть виникнути внаслідок надзвичайних ситуацій. Це дозволяє зберегти робочі місця, зменшити витрати на відновлення та підтримувати стабільний економічний розвиток. Забезпечення цивільної безпеки сприяє соціальній згуртованості та довірі в суспільстві.

Люди, які почуваються безпечно, схильні брати активнішу участь у громадському житті та підтримувати ініціативи, спрямовані на сталий розвиток. Захист навколишнього середовища від техногенних аварій, таких як викиди токсичних речовин або радіаційні інциденти, є важливим елементом цивільної безпеки. Екологічна безпека забезпечує збереження природних ресурсів і біорізноманіття, що є основою сталого розвитку. Цивільна

безпека включає підготовку та адаптацію до змін клімату, які спричиняють підвищення частоти та інтенсивності природних катастроф, таких як повені, урагани та посухи. Адаптаційні заходи дозволяють зменшити вразливість населення і підвищити стійкість громад. Цивільна безпека є невід'ємною частиною стратегії сталого розвитку, яка забезпечує гармонійний розвиток суспільства, економіки та довкілля. Без належного рівня безпеки неможливо досягти сталого прогресу і добробуту для всіх членів суспільства. Ефективне управління та інституційна спроможність є важливими складовими цивільної безпеки. Це включає розробку і реалізацію політик, спрямованих на зниження ризиків і підвищення готовності до надзвичайних ситуацій. Координація між різними рівнями влади, організаціями та громадами сприяє швидкому та ефективному реагуванню на кризи. Підвищення рівня обізнаності населення щодо потенційних загроз і способів їх уникнення є критичним аспектом цивільної безпеки. Освітні програми, тренінги та інформаційні кампанії допомагають людям краще розуміти ризики і підготовуватися до надзвичайних ситуацій. Інформоване населення здатне швидше та ефективніше реагувати на загрози, зменшуючи тим самим їхні негативні наслідки. Загрози цивільній безпеці часто мають глобальний характер, тому міжнародна співпраця є важливим елементом у забезпеченні безпеки. Обмін інформацією, технологіями і досвідом між країнами сприяє розробці ефективних стратегій попередження та реагування на надзвичайні ситуації. Глобальні ініціативи, такі як ООН і міжнародні організації, відіграють ключову роль у координації зусиль і підтримці країн у зміцненні їхньої цивільної безпеки. Сучасні технології і інновації відіграють важливу роль у забезпеченні цивільної безпеки. Використання дронів, штучного інтелекту, систем моніторингу і раннього попередження дозволяє оперативно реагувати на загрози і ефективніше управляти ризиками. Інноваційні підходи до будівництва та інфраструктурних проектів, які враховують принципи стійкості та безпеки, знижують вразливість до природних і техногенних катастроф. Психологічна підтримка для постраждалих від надзвичайних ситуацій є важливим аспектом цивільної безпеки. Забезпечення психологічної допомоги допомагає людям справлятися з наслідками травматичних подій, зберігаючи їхнє психічне здоров'я і здатність до нормального життя та праці.

Соціальні програми та підтримка громади сприяють швидшій реабілітації та інтеграції постраждалих. Інвестиції в проекти цивільної безпеки мають довгострокові економічні вигоди. Витрати на запобігання та підготовку значно нижчі, ніж витрати на ліквідацію наслідків катастроф. Крім того, інвестиції в стійку інфраструктуру і системи безпеки сприяють створенню робочих місць і економічному зростанню. Таким чином, цивільна

безпека є ключовим елементом сталого розвитку, який забезпечує збереження життя, здоров'я і благополуччя населення, стійкість економіки та екосистем. Інтеграція аспектів цивільної безпеки в національні та місцеві стратегії сталого розвитку сприяє створенню безпечних, стійких і процвітаючих громад. Цивільна безпека є основним компонентом сталого розвитку громад, забезпечуючи захист населення, інфраструктури та довкілля. Вона охоплює широкий спектр заходів, спрямованих на зниження ризиків, підвищення стійкості до катастроф та забезпечення благополуччя громад. Розглянемо детальніше, як цивільна безпека сприяє створенню безпечних, стійких і процвітаючих громад. Захист життя та здоров'я громадян є найважливішим завданням цивільної безпеки. Це включає заходи з підготовки до надзвичайних ситуацій, такі як створення планів евакуації, проведення навчань з аварійно-рятувальних робіт та забезпечення доступу до медичної допомоги.

Крім того, безпека інфраструктури – енергетичної, транспортної, водопостачальної та комунікаційної – є критично важливою для підтримки життєдіяльності громади. Цивільна безпека сприяє соціальній стабільності, знижуючи рівень страху та невизначеності серед населення. Коли люди почуваються безпечно, вони більш схильні до активної участі в житті громади, сприяють взаємодопомозі та солідарності. Це підвищує рівень довіри між громадянами та владою, що є основою для створення згуртованого та активного суспільства. Економічна стабільність залежить від здатності громади ефективно управляти ризиками та реагувати на кризи. Цивільна безпека допомагає зменшити економічні втрати від катастроф шляхом впровадження запобіжних заходів та швидкого відновлення після надзвичайних ситуацій. Інвестиції в системи раннього попередження, стійку інфраструктуру та навчання персоналу сприяють довгостроковій економічній стійкості. Збереження довкілля є невід'ємною частиною цивільної безпеки. Заходи, спрямовані на захист екосистем від техногенних аварій, забруднення та інших загроз, допомагають зберегти природні ресурси та біорізноманіття. Крім того, адаптація до змін клімату, включаючи заходи з підготовки до екстремальних погодних умов, сприяє підвищенню стійкості громад до природних катастроф. Підвищення обізнаності населення щодо можливих загроз та методів їх запобігання є важливим аспектом цивільної безпеки [1].

Освітні програми, тренінги та інформаційні кампанії дозволяють громадянам бути краще підготовленими до надзвичайних ситуацій та більш ефективно реагувати на них. Інформоване населення є основою для створення безпечних та стійких громад. Забезпечення психологічної допомоги постраждалим від катастроф допомагає зберегти їхнє психічне здоров'я

та соціальну адаптацію. Соціальні служби, які надають підтримку в кризових ситуаціях, сприяють швидшій реабілітації постраждалих та їх інтеграції в суспільство. Це важливо для підтримки соціальної згуртованості та стабільності в громаді. Цивільна безпека є критичним чинником сталого розвитку безпечних, стійких і процвітаючих громад. Вона забезпечує захист життя та здоров'я населення, підтримує економічну стабільність, зберігає екологічну стійкість та сприяє соціальній згуртованості. Інтеграція аспектів цивільної безпеки в стратегії розвитку громад є необхідною умовою для створення умов, в яких люди можуть жити, працювати та розвиватися у безпеці та добробуті. Вона відіграє важливу роль у захисті життя та здоров'я населення, забезпеченні стійкості інфраструктури, підтримці економічної стабільності, збереженні екологічної безпеки та підвищенні соціальної згуртованості. Інтеграція заходів цивільної безпеки в стратегії розвитку громад сприяє зниженню ризиків і мінімізації наслідків надзвичайних ситуацій, що дозволяє створювати умови для гармонійного розвитку суспільства. Забезпечення цивільної безпеки включає ефективне управління та координацію, підвищення обізнаності населення, впровадження інноваційних технологій та інвестиції в стійку інфраструктуру. Таким чином, цивільна безпека є невід'ємною частиною стратегії сталого розвитку, яка сприяє створенню безпечних, стійких і процвітаючих громад, де люди можуть жити, працювати та розвиватися у безпеці та добробуті.

Цивільна безпека в умовах цифровізації є важливим аспектом політики багатьох країн світу. Кожна країна розробляє свої концепції та стратегії для забезпечення безпеки громадян в цифровому середовищі, враховуючи свої національні особливості, технологічний розвиток і специфіку загроз.

1) Концепція кібербезпеки та захисту критичної інфраструктури США. Національна стратегія кібербезпеки (National Cybersecurity Strategy) включає основні принципи: захист американського народу, американського способу життя та американських інтересів шляхом зміцнення кіберпростору, забезпечення національної стійкості та захисту критичної інфраструктури; підвищення кіберзахисних можливостей, розвиток кіберграмотності, підтримка міжнародного співробітництва.

2) Закон про поліпшення кібербезпеки критичної інфраструктури (CISA Act), мета якого забезпечення захисту ключових секторів, таких як енергетика, фінанси, охорона здоров'я, транспорт і зв'язок; інформаційний обмін між урядом і приватним сектором, розробка та впровадження стандартів кібербезпеки.

3) Стратегія кібербезпеки для цифрового десятиліття країн ЄС, в основі якої Європейська стратегія кібербезпеки (EU Cybersecurity Strategy): зміцнення кіберстійкості, зменшення кіберзагроз та захист цифрової економіки;

спільна відповідь на кіберзагрози, розвиток кіберзахисних можливостей, посилення кіберграмотності громадян.

4) Законодавчі ініціативи, в основі яких Директива про захист мереж та інформаційних систем (NIS Directive), яка зобов'язує країни-члени впроваджувати заходи щодо підвищення безпеки мереж та інформаційних систем; Загальний регламент захисту даних (GDPR), що регулює обробку персональних даних і забезпечує захист приватності громадян.

5) Національна стратегія кібербезпеки Великобританії, в основі якої Національна стратегія кібербезпеки 2021–2025 (National Cyber Security Strategy), головні цілі якої захистити національні інтереси, забезпечити безпеку та добробут громадян, зміцнити економічну стабільність; розробка пріоритетів, що включають інвестиції в кібербезпеку, розвиток нових технологій захисту, підвищення обізнаності та навичок громадян; координація зусиль у боротьбі з кіберзлочинністю, надання консультацій та підтримки організаціям щодо захисту їхніх систем.

6) Кібербезпекова стратегія Японії (Cybersecurity Strategy та захисту критичної інфраструктури, що включає основні напрямки, в основі яких зміцнення національної кіберстійкості, розвиток технологічних інновацій, забезпечення захисту критичної інфраструктури, співпраця з приватним сектором, міжнародне співробітництво, підвищення кіберграмотності.

7) Національна стратегія кібербезпеки Південної Кореї (National Cybersecurity Strategy), яка включає захист національних інтересів, забезпечення безпеки громадян, сприяння економічному розвитку; інвестиції в дослідження та розробки, підвищення рівня кіберграмотності, співпраця з міжнародними партнерами; розробка політик та стандартів кібербезпеки, проведення досліджень та навчання, підтримка національних та міжнародних ініціатив у сфері кібербезпеки.

Ці концепції відображають різні підходи до забезпечення цивільної безпеки в умовах цифровізації, але всі вони підкреслюють важливість співпраці між державними органами, приватним сектором і міжнародними партнерами, а також акцентують увагу на підвищенні рівня обізнаності та підготовки громадян. Серед викликів та загроз виділяємо наступні: 1) Кіберзлочинність: Зростання числа кіберзлочинів, таких як хакерські атаки, фішинг, викрадення особистих даних, що ставить під загрозу приватність та безпеку громадян. 2) Збільшення обсягів зібраних і оброблюваних даних вимагає посилення заходів щодо їх захисту та дотримання принципів конфіденційності. 3) Нерівномірний доступ до цифрових технологій може поглиблювати соціальні та економічні розриви, що негативно впливає на загальний рівень безпеки. 4) Прийняття та оновлення законодавства, що регулює питання кібербезпеки та захисту

персональних даних. 5) Підвищення рівня цифрової грамотності населення через освітні програми та інформаційні кампанії. 6) Впровадження новітніх технологій для захисту від кіберзагроз та забезпечення безпеки цифрових систем. 7) Координація зусиль на міжнародному рівні для боротьби з кіберзлочинністю та обміну передовими практиками у сфері цифрової безпеки.

Таким чином, відмітимо, що цивільна безпека в умовах цифровізації передбачає створення безпечного цифрового середовища, яке захищає громадян від нових ризиків та водночас використовує переваги цифрових технологій для підвищення якості життя та рівня безпеки. Цивільна безпека в умовах цифровізації є комплексним завданням, що вимагає інтегрованого підходу, врахування сучасних викликів та можливостей, які надають цифрові технології. Успішна реалізація концепцій цифрової безпеки базується на балансі між захистом інформаційних систем, збереженням конфіденційності даних та забезпеченням доступу до цифрових технологій для всіх верств населення. Цифровізація приносить значні переваги, але також ставить нові виклики. Ефективне забезпечення цивільної безпеки в умовах цифровізації потребує адаптації до змін, використання передових практик і технологій, а також активної участі всіх зацікавлених сторін. Тільки такий комплексний підхід може забезпечити безпеку, захист прав і свобод громадян у цифровому світі. Таким чином, цивільна безпека має як теоретичне, так і практичне значення, що дозволяє не лише розуміти та прогнозувати загрози, але й ефективно на них реагувати, захищаючи населення та підтримуючи соціальну стабільність, залучаючи цифрові технології до системи цивільної безпеки.

9.7 ПОЛІТИЧНА БЕЗПЕКА

Політична безпека є ключовим аспектом національної безпеки, що охоплює захист політичних інститутів, процесів, ідеологій та державного суверенітету від внутрішніх і зовнішніх загроз. Вона включає в себе стабільність державної влади, законність і прозорість політичних процесів, дотримання прав людини, запобігання політичним конфліктам і екстремізму. Політична безпека стосується захисту від зовнішнього впливу, такого як втручання інших держав у внутрішні політичні справи, інформаційна війна, пропаганда або інші форми гібридної війни, які можуть дестабілізувати країну. У сучасних умовах значне значення має забезпечення кібербезпеки, що захищає політичні структури від кібератак і маніпуляцій у цифровому просторі.

Сучасні виклики політичній безпеці включають зростання популізму, політичну поляризацію, втручання іноземних держав у виборчі процеси, а також використання новітніх технологій для впливу на політичну свідомість громадян. Важливою складовою політичної безпеки є ефективне управління і запобігання корупції, що сприяє довірі громадян до державних інституцій і стабільності політичної системи. Політична безпека тісно пов'язана з іншими аспектами національної безпеки, такими як економічна, військова, соціальна, інформаційна безпека, має фундаментальне значення для збереження державного суверенітету та незалежності.

Політична безпека – стан захищеності політичної системи, державних інститутів, суверенітету та національної ідентичності від внутрішніх і зовнішніх загроз, які можуть дестабілізувати або зруйнувати політичний порядок країни. Ця концепція охоплює захист від впливу інших держав, організацій або окремих осіб, що можуть впливати на політичну стабільність через різноманітні методи, включаючи інформаційну війну, пропаганду, економічний тиск або втручання у внутрішні справи. Політична безпека є важливою складовою національної безпеки, оскільки політична стабільність і суверенітет держави безпосередньо впливають на її здатність забезпечувати безпеку в інших сферах, таких як економіка, оборона та соціальна сфера.

Таблиця 9.34 – Ключові аспекти політичної безпеки

Ключові аспекти	**Зміст та характеристика**
1	2
Стабільність політичної системи	Здатність політичних інститутів ефективно функціонувати без значних змін або загроз дестабілізації. Збереження законності, легітимності та прозорості політичних процесів. Запобігання екстремізму, радикалізму та політичній поляризації.
Захист державного суверенітету	Охорона територіальної цілісності та незалежності держави від зовнішніх загроз. Захист від втручання іноземних держав у внутрішні політичні справи, включаючи інформаційні атаки та пропаганду. Ефективне управління зовнішньою політикою та міжнародними відносинами. Захист державного суверенітету. Забезпечення контролю держави над своєю територією, населенням і ресурсами, а також недопущення втручання з боку інших держав або суб'єктів міжнародного права.
Захист національної ідентичності	Підтримка і розвиток національної культури, мови, релігії та інших аспектів, що формують унікальність нації, а також боротьба проти загроз асиміляції або культурного розмивання.

Закінчення таблиці 9.34

1	2
Політична стабільність державний лад	Недопущення політичних криз, які можуть призвести до переворотів, революцій, громадянських війн або інших форм насильства, що ставлять під загрозу.
Кібербезпека	Захист політичних інститутів і процесів від кібератак, які можуть дестабілізувати державу або вплинути на політичну свідомість громадян. Забезпечення безпеки інформаційних систем, які використовуються в державному управлінні та під час виборів.
Захист конституційного ладу	Забезпечення дотримання Конституції та законів, які регулюють політичну систему. Запобігання спробам узурпації влади або насильницьких змін у політичній системі.
Політична легітимність і довіра громадян	Забезпечення довіри громадян до політичних інститутів через відкриті, прозорі та справедливі виборчі процеси. Боротьба з корупцією та зловживанням владою, які можуть підірвати довіру громадян до держави. Забезпечення участі громадян у політичному житті через механізми демократії.
Інформаційна безпека	Захист від інформаційних атак, дезінформації та пропаганди, що можуть вплинути на політичну стабільність. Розвиток інформаційної грамотності серед населення для запобігання маніпуляціям у ЗМІ та соціальних мережах.
Правове забезпечення політичної безпеки	Розробка і впровадження правової бази, яка регулює політичну діяльність і забезпечує захист від загроз політичній стабільності. Своєчасне оновлення законодавства для адаптації до нових викликів і загроз.
Стабільність політичних інститутів	Підтримання безперервного і ефективного функціонування державних органів, таких як уряд, парламент, судова система, щоб уникнути кризових ситуацій або політичного хаосу.
Правоохоронна та контррозвідувальна діяльність	Робота силових структур, спрямована на виявлення, запобігання і нейтралізацію загроз політичній безпеці, таких як тероризм, екстремізм, шпигунство тощо.
Виборча безпека	Забезпечення чесних і прозорих виборів, що є основою демократичного суспільства, та захист від зовнішнього втручання в цей процес.
Інформаційна безпека	Захист суспільства від маніпуляцій, дезінформації та пропаганди, спрямованих на дестабілізацію внутрішньої ситуації або вплив на політичні процеси.

Складові політичної безпеки можна поділити на кілька основних компонентів, кожен з яких має критичне значення для забезпечення стабільності та стійкості політичної системи. Ці складові політичної безпеки взаємопов'язані й утворюють цілісну систему, яка дозволяє державі ефективно функціонувати, підтримувати стабільність і захищати свої інтереси

як на внутрішньому, так і на міжнародному рівнях. Слід виявити умови, які сприяють забезпеченню політичної безпеки. Органи національної безпеки завжди наполягали на тому, щоб вважати людей основною відправною точкою та опорою забезпечення національної безпеки, що національна безпека – для людей. Безпека в різних галузях взаємопов'язана та впливає одна на одну. Органи національної безпеки завжди дотримувалися загальної концепції національної безпеки як керівництва, приймаючи підтримку політичної безпеки як основне завдання, координуючи та зміцнюючи роботу в традиційних галузях безпеки, таких як військова та внутрішня безпека, та нетрадиційних галузях безпеки, таких як наука та технологія, фінанси та біологія, запобігання та усунення інших областей.

Таблиця 9.35 – Ключові аспекти політичної безпеки

Ключові аспекти	**Зміст та характеристика**
1	2
Сильні інститути	Ефективні державні органи, які здатні виконувати свої функції без втручання ззовні, забезпечують законність і правопорядок, а також захищають права громадян.
Політична культура	Високий рівень політичної культури серед громадян і політичних еліт сприяє вирішенню конфліктів мирними засобами, зміцненню довіри до влади і зменшенню ризиків політичної нестабільності.
Верховенство права	Забезпечення дотримання законів і прав людини, а також справедливість і прозорість у прийнятті політичних рішень.
Незалежна судова система	Судова влада, яка діє незалежно від політичного впливу, забезпечує справедливий розгляд конфліктів і суперечок.
Чесні і прозорі вибори	Проведення виборів без фальсифікацій і втручання з боку зовнішніх або внутрішніх сил сприяє легітимності політичної влади.
Політичний плюралізм	Забезпечення умов для вільної конкуренції політичних партій та організацій, що дозволяє громадянам вільно висловлювати свої політичні переконання.
Соціально-економічна стабільність	Проведення державної політики, спрямованої на забезпечення економічного зростання, зниження рівня безробіття і бідності, що зменшує ризик соціальних потрясінь.
Гнучка зовнішня політика	Підтримка конструктивних відносин з іншими державами і міжнародними організаціями, що сприяє захисту національних інтересів і зменшує ризик зовнішніх загроз.
Захист від пропаганди і дезінформації	Розвиток медіаграмотності серед населення, забезпечення вільного доступу до перевіреної інформації та протидія зовнішнім і внутрішнім інформаційним атакам.
Контроль закіберпростором	Забезпечення кібербезпеки для запобігання втручанню у внутрішні політичні процеси через кіберзагрози.

Закінчення таблиці 9.35

1	2
Соціальна згуртованість	Забезпечення рівних прав і можливостей для всіх громадян, незалежно від їхнього етнічного, релігійного або соціального походження, сприяє зміцненню національної єдності.
Захист національних меншин	Врахування інтересів і прав національних меншин у державній політиці з метою запобігання внутрішнім конфліктам.
Професійна армія і спецслужби	Забезпечення безпеки держави від зовнішніх і внутрішніх загроз шляхом ефективної діяльності військових і правоохоронних органів.
Контррозвідка і боротьба з тероризмом	Своєчасне виявлення та нейтралізація загроз, що можуть дестабілізувати політичну ситуацію в країні.
Участь у міжнародних організаціях	Співпраця з іншими державами у рамках міжнародних організацій, таких як ООН, ОБСЄ, НАТО, сприяє зміцненню політичної безпеки.
Дипломатичні відносини	Розвиток дипломатичних відносин з іншими країнами для захисту національних інтересів і забезпечення підтримки на міжнародній арені.

Забезпечення політичної безпеки вимагає постійної уваги та зусиль з боку держави, суспільства та міжнародної спільноти, оскільки загрози можуть мати динамічний і непередбачуваний характер. Зарубіжний досвід забезпечення політичної безпеки є різноманітним і залежить від політичних, соціальних, культурних та історичних особливостей кожної країни. Без політичної безпеки будь-яка країна неминуче розвалиться на частини, і неможливо буде говорити про її велике відродження чи процвітання. Суверенітет, незалежність та територіальна цілісність є передумовою та основою виживання та розвитку країн, зокрема, народження сучасних національних держав ще більше затвердило основні норми міжнародних відносин, такі як національну рівність, суверенну незалежність, територіальну цілісність, невтручання у внутрішні справи.

Основою політичної безпеки є безпека режиму та системної безпеки. Органи національної безпеки завжди віддавали найвищий пріоритет підтримці політичної безпеки, приймаючи політичну безпеку як головний пріоритет. Зрозуміти природу політичної безпеки людей, це створити фундаментальну гарантію того, щоб люди могли жити та працювати у мирі та достатку.

Підтримка політичної безпеки є фундаментальним інтересом усіх етнічних груп країни. Для цього корисним для нас є зарубіжний досвід забезпечення політичної безпеки.

Таблиця 9.36 – Зарубіжний досвід забезпечення політичної безпеки

Країна	Напрямок забезпечення	Характеристика
1	2	3
США	Розвинена система стримувань і противаг	У Сполучених Штатах система стримувань і противаг між виконавчою, законодавчою і судовою гілками влади забезпечує стабільність політичної системи та запобігає концентрації влади в одних руках.
Інституційна стабільність і національна безпека	Роль спецслужб і правоохоронних органів	США мають потужні правоохоронні органи та розвинену систему національної безпеки, яка включає ЦРУ, ФБР, АНБ та інші агентства, що забезпечують захист держави від внутрішніх і зовнішніх загроз.
Захист критичної інфраструктури та політичних процесів від кіберзагроз	Кібербезпека	Після серії кібернападів у 2000-х роках США посилили кібербезпеку, створивши спеціалізовані підрозділи для захисту критичної інфраструктури та політичних процесів від кіберзагроз.
Німеччина	Конституційний захист	Конституційний суд Німеччини відіграє важливу роль у забезпеченні політичної стабільності, захищаючи демократичний порядок і права громадян. Він може забороняти діяльність екстремістських партій, які загрожують основам конституційного ладу.
Демократичний консенсус і боротьба з екстремізмом	Інтеграція меншин	Німеччина активно працює над інтеграцією мігрантів та національних меншин, що сприяє зменшенню соціальної напруги та підвищенню соціальної згуртованості.
Боротьба з політичним екстремізмом і радикалізацією молоді	Програми протидії екстремізму	У Німеччині існують державні програми, спрямовані на боротьбу з політичним екстремізмом і радикалізацією молоді. Це включає освітні ініціативи, роботу з громадами та посилення правоохоронних заходів.
Велика Британія	Правова держава	Велика Британія має давню традицію правової держави, де верховенство права забезпечується незалежними судами та прозорою системою правосуддя. Це сприяє збереженню політичної стабільності.
Сильна правова система і антишпигунська діяльність	Внутрішня безпека і зовнішня розвідка	Британські служби безпеки MI5 (внутрішня безпека) і MI6 (зовнішня розвідка) відіграють ключову роль у захисті країни від терористичних та шпигунських загроз.

Продовження таблиці 9.36

1	2	3
Запобігання поширенню дезінформації та радикальних ідей	Моніторинг соціальних мереж	Британія активно моніторить соціальні мережі та інтернет-простір для запобігання поширенню дезінформації та радикальних ідей, що можуть загрожувати політичній стабільності.
Франція	Антитерористичні ініціативи	Франція активно бореться з тероризмом через спеціалізовані підрозділи поліції та військових, а також завдяки посиленому законодавству, спрямованому на попередження терористичних атак.
Антитерористичні заходи і соціальна політика	Соціальна інтеграція	Франція проводить політику соціальної інтеграції для зменшення соціальної напруги, особливо серед етнічних і релігійних меншин. Це включає програми освіти, працевлаштування та культурної інтеграції.
Боротьба з дезінформацією та маніпуляціями в медіапросторі	Інформаційна безпека	Франція посилює інформаційну безпеку через законодавчі ініціативи, спрямовані на боротьбу з дезінформацією та маніпуляціями в медіапросторі.
Скандинавські країни	Соціальний контракт	У країнах, таких як Швеція, Норвегія та Данія, існує високий рівень соціальної згуртованості та довіри до уряду, що сприяє стабільності політичної системи. Державна політика спрямована на забезпечення соціальної рівності та підтримку добробуту всіх громадян.
Соціальна згуртованість і довіра до уряду	Гармонізація між етнічними групами	Скандинавські країни активно працюють над інтеграцією етнічних меншин та мігрантів, запобігаючи соціальним конфліктам і підтримуючи стабільність.
Високий рівень політичної участі	Політична участь	Високий рівень політичної участі громадян, прозорість урядових процесів і доступність політичного діалогу є ключовими факторами, що забезпечують політичну безпеку в Скандинавії.
Ізраїль	Обов'язкова військова служба	В Ізраїлі обов'язкова військова служба сприяє високому рівню підготовленості населення до захисту країни, що є важливим фактором політичної безпеки.
Комплексна безпека і громадянська відповідальність	Розвинена розвідка	Ізраїль має одну з найпотужніших розвідувальних служб у світі – Моссад, яка відіграє ключову роль у запобіганні зовнішніх і внутрішніх загроз.

Закінчення таблиці 9.36

1	2	3
Висока національна єдність	Національна єдність	В умовах постійних зовнішніх загроз Ізраїль зумів побудувати високу національну єдність, де громадяни відчувають відповідальність за захист держави.
Сінгапур	Жорсткий контроль над політичним процесом	Сінгапур має авторитарну модель управління, де політичний процес контролюється владою для забезпечення стабільності. Хоча це викликає критику з боку правозахисних організацій, цей підхід допоміг країні уникнути політичних потрясінь.
Авторитарний підхід і економічна стабільність	Економічний розвиток	Сінгапур активно інвестує в економічний розвиток, що сприяє підвищенню рівня життя громадян і зменшенню соціальної напруги.
Підтримка політичної стабільності	Закони проти расової та релігійної ненависті	У Сінгапурі діють суворі закони проти розпалювання расової та релігійної ненависті, що сприяє підтримці політичної стабільності в багатонаціональному суспільстві.

Таблиця 9.36 – (власне джерело)

Ці приклади демонструють різні підходи до забезпечення політичної безпеки, але можуть бути корисними для вивчення та адаптації досвіду. аїнах. Кожна країна вибудовує свою систему політичної безпеки на основі власних викликів, ресурсів і національних особливостей. Політична безпека – це стан, у якому національна влада, політична система, політичний порядок та ідеологія захищені від загроз, порушень, підривної діяльності та руйнування. Це основна сфера національної безпеки, в основі якої є безпека режиму та системної безпеки. Політична безпека є ключовим аспектом національної безпеки, що передбачає захист держави від внутрішніх та зовнішніх загроз, які можуть підірвати політичну стабільність, суверенітет і демократичні інститути. Зарубіжний досвід у сфері політичної безпеки включає різноманітні заходи та програми, які країни впроваджують для зміцнення своєї політичної системи та захисту від загроз.

Після втручання у президентські вибори 2016 року, США запровадили комплексну програму кібербезпеки для захисту виборчої інфраструктури. Вона включає розробку стандартів безпеки, підвищення кіберобізнаності серед виборчих органів, співпрацю з приватним сектором і міжнародними партнерами для забезпечення прозорості та захищеності виборчих процесів. Агентство з кібербезпеки та інфраструктурної безпеки (CISA) відповідає за захист критичної інфраструктури, включаючи виборчі системи, від

кіберзагроз. CISA також працює над протидією дезінформації та фальсифікаціям, які можуть вплинути на виборчі процеси та довіру громадськості.

Ізраїль сформував концепцію зміцнення національної безпеки та політичної стабільності. Ізраїльська служба внутрішньої безпеки "Shin Bet" (Шабак) відповідає за захист політичної системи та боротьбу з тероризмом. Вона активно займається контррозвідувальною діяльністю, запобіганням внутрішнім загрозам і захистом державних лідерів. Shin Bet також контролює екстремістські організації, що можуть загрожувати політичній стабільності. Ізраїльські програми по боротьбі з тероризмом включають комплексні заходи з протидії терористичним актам, що можуть мати політичний характер. Це включає аналітичну роботу, роботу з громадами та заходи, спрямовані на мінімізацію радикалізації.

Франція сформувала концепцію протидії радикалізації та захист світської держави. Після серії терористичних атак у Франції, уряд розробив національний план протидії радикалізації, що спрямований на запобігання впливу екстремістських ідей на населення. План включає освітні програми, підтримку сімей, соціальні ініціативи та роботу з місцевими громадами для виявлення і запобігання радикалізації на ранніх етапах. Франція також активно захищає свої світські цінності через законодавчі ініціативи, спрямовані на обмеження впливу релігійних організацій на політичні процеси. Це включає заборону релігійної символіки у державних установах та освітніх закладах, що допомагає підтримувати нейтральність держави.

Німеччина сформувала концепцію захисту від екстремізму та захисту демократичного ладу. Федеральне управління з охорони конституції (BfV) відповідає за внутрішню безпеку Німеччини, зокрема за захист демократичного ладу від екстремістських рухів та організацій. BfV займається моніторингом політичних екстремістів, терористичних організацій, а також іноземних розвідувальних служб, що можуть впливати на політичну стабільність країни. Після зростання ультраправих настроїв у Німеччині, уряд розробив спеціальні програми для протидії екстремізму, які включають моніторинг соціальних мереж, роботу з молоддю та підтримку проектів, спрямованих на підвищення політичної обізнаності та толерантності.

Велика Британія сформувала концепцію протидії тероризму та захисту публічного простору. Частина національної стратегії протидії тероризму Великої Британії, програма "PREVENT" спрямована на запобігання радикалізації і залученню людей до терористичних організацій. Вона включає освітні програми, співпрацю з громадами, роботу з вразливими групами населення та підтримку ініціатив, що сприяють інтеграції. Уряд Великої Британії розробляє заходи для захисту публічного простору від терористичних атак,

зокрема через встановлення фізичних бар'єрів, посилення спостереження і підвищення готовності сил безпеки до можливих нападів.

Сінгапур сформував комплексний підхід до національної безпеки, реалізує комплексну програму під назвою "Total Defence", яка охоплює п'ять основних аспектів: військову, цивільну, економічну, соціальну та психологічну оборону. Ця програма забезпечує всебічну готовність держави та громадян до різних загроз, включаючи політичні загрози та дезінформацію. В умовах зростання загроз інформаційної війни Сінгапур впроваджує заходи для боротьби з дезінформацією та фальсифікаціями, що можуть підірвати політичну стабільність. Це включає освітні програми, законодавчі ініціативи та активну роль уряду у спростуванні неправдивої інформації.

Зарубіжний досвід свідчить, що для забезпечення політичної безпеки держави використовують широкий спектр заходів, які включають кібербезпеку, контррозвідувальні операції, боротьбу з тероризмом, протидію радикалізації та дезінформації, а також захист демократичних інститутів і прав людини. Ці програми та ініціативи допомагають зберігати політичну стабільність і стійкість до різних загроз, що є ключовими для національної безпеки.

Сьогодні штучний інтелект ставить нові виклики політичній безпеці. Технологічні зміни мають дві сторони. Штучний інтелект – це одночасно нова можливість та новий виклик для підтримки політичної безпеки. Одна із проблем: популяризація та застосування технологій штучного інтелекту призвели до тенденції «децентралізації» політичної влади. У період розвитку штучного інтелекту дані уособлюють силу, суб'єктами, які контролюють дані, є органи державної влади, а також недержавні суб'єкти, такі як окремі особи, бізнес-групи та громадські організації. «Багатовузловий, безцентровий» дизайн структури «Інтернет-даних» визначає, що суб'єкти, які займають будь-яку позицію в онлайн-спільноті, не можуть мати більшого статусу, ніж суб'єкти, що займають інші позиції. Ця особливість послаблює традиційну офлайнову бюрократичну структуру національного управління та односторонню модель управління, а також владу політичного дискурсу.

Оскільки технології штучного інтелекту та монополія на дані продовжують розширюватись, то й розширення влади капіталу ставить під загрозу межі національної влади. Розвиток та зміни продуктивних сил неминуче спричинять коригування виробничих відносин, включаючи структуру політичної влади. Коли технологія штучного інтелекту широко використовуватиметься в різних економічних та соціальних галузях і викликатиме зміни, це сприятиме відповідним коригуванням структури національного управління та моделі розподілу влади. З іншого боку, потужна стимулююча роль технологій штучного інтелекту та перспективи

її економічного та соціального застосування призвели до перетікання в неї капіталу. В епоху штучного інтелекту гігантські компанії, що спираються на сильний капітал, поступово монополізують технології та контролюють дані. Технологія штучного інтелекту, а також дані та алгоритми, що лежать в її основі, тонко спрямовують громадську думку, впливаючи на політичні міркування та вибір людей та опосередковано контролюючи політичні тенденції. В епоху штучного інтелекту дані та алгоритми – це нова сила. Різні політичні операції, пов'язані з національними виборами в останні роки, показали, що наявність даних та технологій може певною мірою впливати на політичний порядок денний.

Технології штучного інтелекту можуть використовуватись політично ворожими силами для здійснення проникнення, підривної діяльності, диверсій та сепаратистської діяльності. Існує безліч прикладів використання передових технологій для загрози політичній безпеці інших країн. Після появи комп'ютерних мережевих технологій вони почали використовувати зловмисниками для реалізації кіберкрадіжки, кібератак, кіберзмови, поширення політичних чуток, ідеологічного проникнення і атак. В епоху штучного інтелекту наслідки атаки на систему штучного інтелекту країни або використання штучного інтелекту для здійснення проникнення, підривної, диверсійної та сепаратистської діяльності є серйознішими, ніж раніше. Розвиток технологій штучного інтелекту створює серйозні проблеми участі суверенних країн у міжнародній конкуренції. Штучний інтелект в даний час є однією з передових технологій, а його основні технології в основному освоєні розвиненими країнами, такими як США та Європа. Ці країни використовують його для підвищення рівня автоматизації виробництва, підвищення продуктивності праці та прискорення переміщення обробних виробництв. Необхідно підвищувати обізнаність про ризики, уважно стежити за розвитком технологій та програмами штучного інтелекту, регулярно вивчати та оцінювати політичні ризики, які може принести штучний інтелект, а також покращувати можливості виявлення, запобігання та усунення ризиків.

В даний час найбільш серйозною загрозою безпеці, з якою стикаються високорозвинені країни в галузі технологій штучного інтелекту, є те, що ключові базові технології контролюються іншими. Необхідно мобілізувати зусилля всіх країн для створення низки національних платформ досліджень та розробок у галузі штучного інтелекту, починаючи з інтелектуальних – чіпи, базові алгоритми, ключові компоненти, високоточні датчики і т. д., щоб прискорити розвиток платформ досліджень та розробок у галузі штучного інтелекту. Враховуючи ризики застосування технологій, для забезпечення здорового розвитку штучного інтелекту

необхідні суворе формулювання стандартів штучного інтелекту та галузевий нагляд. Активізувати зусилля щодо вдосконалення законів, правил та етичних норм, пов'язаних із штучним інтелектом, прояснити відповідні питання, такі як підтвердження цивільної та кримінальної відповідальності, захист конфіденційності та прав власності, а також машинна етика, а також упорядкувати права та обов'язки серед дизайнерів, користувачів, та регулятори. Необхідно створити та вдосконалити систему нагляду за штучним інтелектом, реалізувати нагляд за всім процесом проектування алгоритмів, розробки продуктів та застосування результатів. Необхідно активно досліджувати та вивчати теорію інтелектуальної війни, прискорити створення сучасних систем озброєння та техніки та талановитих команд, посилити підготовку та навчання військ в інтелектуальних умовах, а також постійно підвищувати рівень готовності армії до військової боротьби в умовах війни.

9.8 ЕКОЛОГО-ПРАВОВІ АСПЕКТИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Актуальність дослідження еколого-правових аспектів національної безпеки України в умовах воєнного стану набуває особливого значення, оскільки зростають екологічні загрози у зв'язку з воєнними діями на території України, що призводять до значних руйнувань інфраструктури, промислових та цивільних об'єктів, забруднення довкілля, серйозних ризиків для здоров'я населення і стійкості екосистем. Існує потреба в адаптації та вдосконаленні національного законодавства для забезпечення належного рівня екологічної безпеки в умовах воєнного стану, що обумовлено розробкою нових норм і правил, які враховують специфіку воєнних умов [44]. Екологічна безпека є складовою частиною національної безпеки. Пошкодження екосистем і природних ресурсів може мати довгострокові наслідки для економіки, здоров'я населення та соціальної стабільності, що вимагає комплексного наукового аналізу. Україна має виконувати свої міжнародні зобов'язання у сфері охорони довкілля, навіть у складних умовах воєнного часу, мають розроблені стратегії для забезпечення екологічної безпеки у відповідності до міжнародних стандартів. Для успішного відновлення України після війни необхідно мати чітке розуміння екологічних наслідків воєнних дій та розробити плани з відновлення і рекультивації постраждалих територій [45].

Метою дослідження еколого-правових аспектів національної безпеки України в умовах воєнного стану є забезпечення комплексного

підходу щодо: аналізу та оцінки впливу воєнних дій на масштаби та характер екологічних загроз, спричинених воєнними діями, зокрема забруднення ґрунтів, водних ресурсів, повітря та біорізноманіття; оцінки ефективності чинного екологічного законодавства щодо захисту довкілля в умовах воєнного стану; формування науково обґрунтованих підходів до екологічного відновлення та рекультивації територій, що постраждали від воєнних дій, з урахуванням міжнародного досвіду; визначення ролі екологічної безпеки як ключового елемента національної безпеки, та інтегрувати екологічні аспекти у загальну стратегію захисту та розвитку України.

В табл. 9.37 проведено аналіз та оцінка факторів впливу воєнних дій на довкілля, що спричиняють масштабні та різноманітні екологічні загрози.

Таблиця 9.37 – Фактори впливу воєнних дій (бомбардування, артилерійські обстріли, вибухи тощо) на масштаби та характер екологічних загроз

Наслідки воєнних дій	**Масштаби та характер екологічних загроз**
1	2
1. Забруднення ґрунтів	Токсичні речовини: – викиди хімічних речовин з боєприпасів, – руйнування промислових об'єктів, сховищ пального та хімікатів призводять до забруднення ґрунтів важкими металами, нафтопродуктами та іншими токсинами. Наслідки для сільського господарства: – забруднення ґрунтів може робити великі площі непридатними для ведення сільського господарства, що впливає на продовольчу безпеку.
2. Забруднення водних ресурсів	Пошкодження інфраструктури: – руйнування водоочисних споруд, гребель, хімічних підприємств призводить до витоків токсичних речовин у річки, озера, підземні води. Забруднення поверхневих вод: – через бомбардування або обстріли може відбутися забруднення річок та водойм хімікатами, нафтопродуктами, які важко очищуються та мають тривалий негативний вплив на екосистеми.
3. Забруднення повітря	Викиди від вибухів: – вибухи боєприпасів, руйнування інфраструктури викликають викиди пилу, диму, важких металів, діоксинів та інших шкідливих речовин у повітря. Руйнування лісових масивів: – пожежі внаслідок обстрілів або бомбардувань спричиняють великі викиди вуглекислого газу та інших продуктів горіння, що погіршує якість повітря і сприяє глобальному потеплінню.

Закінчення таблиці 9.37

1	2
4. Вплив на біорізноманіття	Знищення середовищ існування: – військові операції можуть знищувати природні середовища проживання тварин та рослин, що веде до втрати біорізноманіття; – загибель флори і фауни; – забруднення ґрунтів, води та повітря, а також пряме фізичне руйнування екосистем призводить до загибелі багатьох видів тварин і рослин, зокрема рідкісних і зникаючих. Порушення міграційних шляхів: – військові дії можуть порушувати природні міграційні шляхи птахів, риб та інших видів, що ускладнює їх виживання.
5. Довгострокові наслідки	Збереження токсинів у довкіллі: – багато токсичних речовин можуть залишатися в ґрунтах та водних ресурсах десятиліттями, поступово накопичуючись у ланцюгу живлення. Порушення екологічного балансу: – тривалі екологічні зміни можуть призводити до порушення екологічного балансу в регіонах, що впливає на клімат, здоров'я людей та економічний розвиток.

Таблиця 9.37 – (власне джерело)

Таким чином, вплив воєнних дій на довкілля є надзвичайно масштабним і має серйозні наслідки для екологічної безпеки України. Важливо проводити детальний аналіз і моніторинг цих загроз, розробляти правові та технічні заходи для їх мінімізації, а також залучати міжнародні ресурси для відновлення екосистем після завершення бойових дій.

На законодавчому рівні екологічні аспекти національної безпеки України в умовах воєнного стану закріплено в ряді нормативно-правових актів, що регулюють діяльність у сфері оборони, екології та забезпечення безпеки національного рівня; визначають норми та принципи охорони навколишнього середовища, регулюють взаємодію органів влади, громадськості та підприємств у сфері екології та безпеки [46]

Конституція України статтею 16 визначає, що «обов'язком держави є забезпечення екологічної безпеки і підтримання екологічної рівноваги на території України, подолання наслідків катастрофи планетарного масштабу, збереження генофонду українського народу; стаття 50 визначає право кожного на безпечне для життя і здоров'я довкілля та на відшкодування завданої порушенням цього права шкоди; право вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення» [47].

Еколого-правові аспекти національної безпеки України в умовах воєнного стану мають особливе значення через комплексний вплив військових дій на довкілля та необхідність адаптації правових механізмів для його захисту.

Україна має низку законів, спрямованих на захист довкілля, які залишаються актуальними під час воєнного стану [48]:

Закон України «Про охорону навколишнього природного середовища» визначає правові, економічні та соціальні основи організації охорони навколишнього природного середовища в інтересах нинішнього і майбутніх поколінь». У статті 9 зазначено, що кожний громадянин України має право на [49]:

а) безпечне для його життя та здоров'я навколишнє природне середовище;

б) участь в обговоренні та внесення пропозицій до проектів нормативно-правових актів, матеріалів щодо розміщення, будівництва і реконструкції об'єктів, які можуть негативно впливати на стан навколишнього природного середовища, внесення пропозицій до органів державної влади та органів місцевого самоврядування, юридичних осіб, що беруть участь в прийнятті рішень з цих питань;

в) участь в розробці та здійсненні заходів щодо охорони навколишнього природного середовища, раціонального і комплексного використання природних ресурсів;

г) здійснення загального і спеціального використання природних ресурсів;

д) об'єднання в громадські природоохоронні формування;

е) вільний доступ до інформації про стан навколишнього природного середовища (екологічна інформація) та вільне отримання, використання, поширення та зберігання такої інформації, за винятком обмежень, встановлених законом;

є) участь у громадських обговореннях з питань впливу планованої діяльності на довкілля;

ж) одержання екологічної освіти;

з) подання до суду позовів до державних органів, підприємств, установ, організацій і громадян про відшкодування шкоди, заподіяної їх здоров'ю та майну внаслідок негативного впливу на навколишнє природне середовище;

и) оскарження у судовому порядку рішень, дій або бездіяльності органів державної влади, органів місцевого самоврядування, їх посадових осіб щодо порушення екологічних прав громадян у порядку, передбаченому законом;

і) участь у процесі здійснення стратегічної екологічної оцінки.

Розділ XI Закону передбачає заходи щодо забезпечення екологічної безпеки, зокрема, в статті 50 закріплено поняття «екологічної безпеки як такий стан навколишнього природного середовища, за якого забезпечується попередження погіршення екологічної обстановки та виникнення небезпеки для здоров'я людей. Стаття 58 розкриває вимоги екологічної безпеки щодо військових, оборонних об'єктів та військової діяльності» [50].

Закон України «Про правовий режим воєнного стану», який дозволяє вносити зміни в екологічні норми для швидкого реагування на нові виклики, «визначає зміст правового режиму воєнного стану, порядок його введення та скасування, правові засади діяльності органів державної влади, військового командування, військових адміністрацій, органів місцевого самоврядування, підприємств, установ та організацій в умовах воєнного стану, гарантії прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб». Згідно Закону «воєнний стан – це особливий правовий режим, що вводиться в Україні або в окремих її місцевостях у разі збройної агресії чи загрози нападу, небезпеки державній незалежності України, її територіальній цілісності та передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності, а також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень» [51].

Закон України «Про національну безпеку України» визначає «основи та принципи національної безпеки і оборони, цілі та основні засади державної політики, що гарантуватимуть суспільству і кожному громадянину захист від загроз. Одним із принципів державної політики у сферах національної безпеки і оборони, згідно статті 13, п. 1 є «спрямованість на захист: людини і громадянина – їхніх життя і гідності, конституційних прав і свобод, безпечних умов життєдіяльності; суспільства – його демократичних цінностей, добробуту та умов для сталого розвитку; держави – її конституційного ладу, суверенітету, територіальної цілісності та недоторканності; території, навколишнього природного середовища – від надзвичайних ситуацій». Стаття 3, п. 4 Закону розкриває принцип державної політики у сферах національної безпеки і оборони, який спрямовано на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями». У статті 13, п. 14 зазначено, що керівництво у сферах національної безпеки і оборони приймає у разі необхідності

рішення про введення в Україні або в окремих її місцевостях надзвичайного стану, а також оголошує у разі необхідності окремі місцевості України зонами надзвичайної екологічної ситуації з наступним затвердженням цих рішень Верховною Радою України [52].

Закон України «Основні засади (стратегія) державної екологічної політики України на період до 2030 року» визначає існуючі проблеми та сучасний стан довкілля в Україні; мету, засади, принципи та інструменти державної екологічної політики; стратегічні цілі та завдання державної екологічної політики; етапи реалізації державної екологічної політики; моніторинг та систему показників оцінки реалізації державної екологічної політики, орієнтованих на індикатори сталого розвитку та завдання збалансованої екологічної політики [53]. Згідно Стратегії першопричинами екологічних проблем України є:

– підпорядкованість екологічних пріоритетів економічній доцільності; неврахування наслідків для довкілля у законодавчих та нормативно-правових актах, зокрема у рішеннях Кабінету Міністрів України та інших органів виконавчої влади;

– переважання ресурсо- та енергоємних галузей у структурі економіки із здебільшого негативним впливом на довкілля, що значно посилюється через неврегульованість законодавства при переході до ринкових умов господарювання;

– фізичне та моральне зношення основних фондів у всіх галузях національної економіки;

– неефективна система державного управління у сфері охорони навколишнього природного середовища та регулювання використання природних ресурсів, зокрема неузгодженість дій центральних і місцевих органів виконавчої влади та органів місцевого самоврядування, незадовільний стан системи державного моніторингу навколишнього природного середовища;

– низький рівень розуміння в суспільстві пріоритетів збереження довкілля та переваг збалансованого (сталого) розвитку, недосконаліть системи екологічної освіти та просвіти;

– незадовільний рівень дотримання природоохоронного законодавства та екологічних прав і обов'язків громадян;

– незадовільний контроль за дотриманням природоохоронного законодавства та незабезпечення невідворотності відповідальності за його порушення;

– недостатнє фінансування з державного та місцевих бюджетів природоохоронних заходів, фінансування таких заходів за залишковим принципом [54].

Державна екологічна політика України спрямована на досягнення кількох стратегічних цілей, які мають забезпечити екологічну безпеку, стале використання природних ресурсів та покращення якості життя населення [55].

Ціль 1. Формування в суспільстві екологічних цінностей і засад сталого споживання та виробництва.

Ціль 2. Забезпечення сталого розвитку природно-ресурсного потенціалу України.

Ціль 3. Забезпечення інтеграції екологічної політики у процес прийняття рішень щодо соціально-економічного розвитку України.

Ціль 4. Зниження екологічних ризиків з метою мінімізації їх впливу на екосистеми, соціально-економічний розвиток та здоров'я населення.

Ціль 5. Удосконалення та розвиток державної системи природоохоронного управління.

Стратегічні цілі спрямовані на створення умов для екологічно безпечного та сталого розвитку України, що забезпечить збереження природного середовища для майбутніх поколінь (рис. 9.1).

Закон України «Про охорону атмосферного повітря» спрямований на «збереження та відновлення природного стану атмосферного повітря, створення сприятливих умов для життєдіяльності, забезпечення екологічної безпеки та запобігання шкідливому впливу атмосферного повітря на здоров'я людей та навколишнє природне середовище. Закон визначає правові і організаційні основи та екологічні вимоги в галузі охорони атмосферного повітря». Згідно статті 4 «нормування в галузі охорони атмосферного повітря проводиться з метою встановлення комплексу обов'язкових норм, правил, вимог до охорони атмосферного повітря від забруднення та забезпечення екологічної безпеки та спрямоване на [56]: забезпечення безпечного навколишнього природного середовища та запобігання екологічним катастрофам; реалізацію єдиної науково-технічної політики в галузі охорони атмосферного повітря; встановлення єдиних вимог до обладнання і споруд щодо охорони атмосферного повітря від забруднення; забезпечення безпеки господарських об'єктів і запобігання виникненню аварій та техногенних катастроф; впровадження і використання сучасних екологічно безпечних технологій». Закон України «Про охорону атмосферного повітря» є ключовим інструментом для забезпечення екологічної безпеки та захисту здоров'я населення від шкідливого впливу забруднення повітря. Він стимулює впровадження сучасних технологій очищення викидів, посилює контроль за дотриманням екологічних норм і забезпечує участь громадськості в питаннях охорони довкілля.

Закон України «Про управління відходами» в умовах воєнного є надзвичайно цінним не лише в контексті адаптації екологічного законодавства

1. Забезпечення екологічної безпеки

- *Попередження екологічних катастроф*: прийняття заходів для запобігання аварій, пов'язаних із промисловою діяльністю, військовими діями та стихійними лихами.
- *Зниження забруднення довкілля*: реалізація програм зменшення викидів забруднюючих речовин у повітря, воду та ґрунт, контроль за рівнем радіації та токсичних речовин.
- *Реагування на екологічні загрози*: створення систем швидкого реагування на екологічні інциденти, включаючи вдосконалення законодавства та механізмів моніторингу.

2. Раціональне використання природних ресурсів

- *Сталий розвиток*: забезпечення балансу між використанням природних ресурсів та їх відновленням, щоб зберегти екосистеми для майбутніх поколінь.
- *Ефективне управління ресурсами: в*провадження сучасних технологій для зменшення негативного впливу на довкілля та підвищення ефективності використання ресурсів, таких як вода, ліси, земля і корисні копалини.

3. Покращення якості довкілля та здоров'я населення

- *Забезпечення доступу до чистої води та повітря*: впровадження заходів для забезпечення високої якості питної води та зниження рівня забруднення повітря, особливо в урбанізованих зонах.
- *Охорона здоров'я населення*: зниження впливу шкідливих екологічних факторів на здоров'я людей через підтримку екологічно чистих умов проживання.

4. Збереження біорізноманіття та природних екосистем

- *Охорона природних територій*: створення та розширення мережі природоохоронних територій, національних парків та заповідників для збереження біорізноманіття.
- *Збереження рідкісних видів тварин*: впровадження програм захисту та відновлення видів, які перебувають під загрозою зникнення.

5. Адаптація до зміни клімату

- *Зниження впливу зміни клімату*: розробка заходів для пом'якшення наслідків зміни клімату, таких як зменшення викидів парникових газів і підвищення стійкості до екстремальних погодних умов.
- *Інтеграція кліматичної політики*: включення аспектів адаптації до зміни клімату в усі галузі економіки та суспільного життя.

Рисунок 9.1 – Основні стратегічні цілі державної екологічної політики, які мають забезпечити екологічну безпеку, стале використання природних ресурсів та покращення якості життя населення

України до європейських стандартів охорони навколишнього середовища та поводження з відходами, а й є важливою гарантією захисту екологічних прав, прав громадян, зокрема права на свободу доступу до екологічної інформації. «Закон визначає правові, організаційні, економічні засади діяльності щодо запобігання утворенню, зменшення обсягів утворення

відходів, зниження негативних наслідків від діяльності з управління відходами, сприяння підготовці відходів до повторного використання, рециклінгу і відновленню з метою запобігання їх негативному впливу на здоров'я людей та навколишнє природне середовище» [57].

Закон України «Про внесення змін до деяких законодавчих актів України щодо державної системи моніторингу довкілля, інформації про стан довкілля (екологічної інформації) та інформаційного забезпечення управління у сфері довкілля» містить положення, які стосуються встановлення процедур та вимог щодо збору, обробки та надання екологічної інформації; регламентації функцій та повноважень органів, що здійснюють моніторинг довкілля та забезпечують інформаційне забезпечення управління в цій сфері; визначення вимог до системи моніторингу та методології оцінки стану довкілля; встановлення прав та обов'язків суб'єктів, що здійснюють моніторинг та надання екологічної інформації [58].

Кодекс цивільного захисту України визначає основні принципи та завдання цивільного захисту, включаючи заходи щодо захисту населення та довкілля від можливих небезпек; «регулює відносини, пов'язані із захистом населення, територій, навколишнього природного середовища та майна від надзвичайних ситуацій, реагуванням на них, функціонуванням єдиної державної системи цивільного захисту» [59]. Водний кодекс України регулює використання та охорону водних ресурсів, включаючи заходи для забезпечення безпеки водних об'єктів. «Водний кодекс, в комплексі з заходами організаційного, правового, економічного і виховного впливу, сприятиме формуванню водно-екологічного правопорядку і забезпеченню екологічної безпеки населення України, а також більш ефективному, науково обґрунтованому використанню вод та їх охороні від забруднення, засмічення та вичерпання» [60].

Міжнародні угоди відіграють ключову роль у формуванні еколого-правових аспектів національної безпеки України в умовах воєнного стану, глобальної екологічної політики та зобов'язують Україну дотримуватися певних екологічних стандартів у забезпеченні сфері охорони довкілля:

1. Женевська конвенція про захист цивільного населення під час війни (Четверта Женевська конвенція від 12 серпня 1949 року) визначає правовий захист цивільних осіб під час збройних конфліктів. Цей документ є основою міжнародного гуманітарного права, що регулює правила ведення війни з метою захисту людей, які не беруть участі в бойових діях [61].

2. Додатковий протокол (Протокол I, від 08.06.1977 року) до Женевських конвенцій, що стосується захисту жертв міжнародних збройних конфліктів при веденні воєнних дій. У Статті 55 «Захист природного середовища» прописано, що «при веденні воєнних дій має бути

виявлена турбота про захист природного середовища від широкої, довгочасної і серйозної шкоди. Такий захист включає заборону використання методів або засобів ведення війни, що мають на меті завдати або, як можна очікувати, завдадуть такої шкоди природному середовищу й тим самим завдадуть шкоди здоров'ю або виживанню населення. Заподіяння шкоди природному середовищу як репресалій заборонено» [62].

3. Конвенція про заборону військового або будь-якого іншого ворожого використання засобів впливу на природне середовище, прийнята у 1976 році під егідою ООН (Environmental Modification Convention або ENMOD) – один з основних документів ООН, що запобігання використанню техногенних засобів впливу на навколишнє середовище з військовою метою або з іншими ворожими намірами. Конвенція забороняє воєнні дії, спрямовані на зміну клімату, структури Землі, включно з її біотою, літосферою, гідросферою, атмосферою або космічним простором, землетрусів, цунамі або інших природних явищ для досягнення військових цілей [63]. Україна, як учасник Конвенції, зобов'язується не використовувати засоби впливу на природне середовище для військових цілей, що є важливим для захисту національної безпеки та запобігання екологічним катастрофам. Дотримання положень Конвенції також є важливим для збереження міжнародної репутації України та для співпраці з іншими країнами у сфері охорони довкілля. Враховуючи екологічні ризики, пов'язані з військовими діями, виконання положень Конвенції сприяє мінімізації шкоди довкіллю та захисту природних ресурсів України.

4. Конвенція про заборону або обмеження застосування конкретних видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень або мають невибіркову дію [64], відома також як Конвенція про конкретні види звичайної зброї ООН (Convention on Certain Conventional Weapons, CCW), була прийнята 10 жовтня 1980 року і набула чинності 2 грудня 1983 року. Ця конвенція є важливою складовою міжнародного гуманітарного права, спрямованого на обмеження впливу збройних конфліктів на цивільне населення і навколишнє середовище. Метою Конвенції є обмеження або заборона застосування певних видів звичайної зброї, які можуть завдавати надмірних ушкоджень або мають невибіркову дію, тобто таких, що не можуть розрізняти між комбатантами і некомбатантами.

Конвенція складається з декількох додаткових протоколів, кожен з яких стосується конкретного виду зброї:

Протокол I (1980 р.) – заборона застосування осколкової зброї, що не піддаються виявленню в тілі під час рентгенівського обстеження.

Протокол II (1999 р.) – обмеження застосування мін, мін-пасток та інших пристроїв, спрямованих проти людей.

Протокол III (1980 р.) – заборона або обмеження застосування запалювальної зброї, включаючи напалм, що спричиняє особливо важкі травми або великі руйнування.

Протокол IV (1995 р.) – заборона застосування засліплюючої лазерної зброї.

Протокол V (2003 р.) – забезпечення заходів щодо знешкодження вибухонебезпечних предметів – наслідків війни (снарядів, мін та іншої вибухової зброї, яка не спрацювала).

Участь України в CCW є важливою для забезпечення захисту цивільного населення від наслідків використання невибіркової зброї під час збройних конфліктів. Виконання положень Конвенції та її протоколів сприяє мінімізації шкоди, завданої цивільним особам та навколишньому середовищу. Зокрема, Протокол II про міни є особливо важливим для України, оскільки країна стикається з проблемою замінованих прифронтових територій, що становить серйозну загрозу для населення та ускладнює післявоєнне відновлення. Протокол V регулює заходи щодо очищення територій України від невибухлих снарядів та інших небезпечних предметів, які можуть призводити до жертв серед цивільного населення навіть після закінчення активних бойових дій.

5. Рамкова конвенція Організації Об'єднаних Націй про зміну клімату – екологічний договір, метою якого є стабілізація концентрації парникових газів в атмосфері на рівні, який запобігає небезпечному антропогенному впливу на кліматичну систему. Україна ратифікувала цю конвенцію в 1996 році і виконує зобов'язання щодо зниження викидів парникових газів [65].

6. Кіотський протокол до Рамкової конвенції ООН, прийнятий у 1997 році, про зміну клімату встановлює конкретні кількісні зобов'язання для розвинених країн і країн з перехідною економікою щодо скорочення викидів парникових газів (ратифіковано в Україні у 2004 році) [66].

Таким чином, дослідження еколого-правових аспектів національної безпеки України в умовах воєнного стану сприяє формуванню науково-обґрунтованих підходів до екологічного відновлення та рекультивації територій, що постраждали від воєнних дій, та є важливим етапом у забезпеченні сталого розвитку та відновленні України після завершення військових дій.

Основними напрямками Концепції зелених технологій та стратегій сталого розвитку як чинників забезпечення національної безпеки та збереження навколишнього середовища з метою екологічного відновлення та рекультивації є [67]:

- проведення детального екологічного моніторингу та оцінки стану довкілля на постраждалих територіях, включаючи моніторинг якості повітря, стану вод суші, аналіз забруднення ґрунтів, прибережних вод,

стану ґрунтів, показників біологічного різноманіття, радіаційного випромінювання, а також вивчення інформаційної взаємодії [68];

• використання сучасних дистанційних методів зондування та геоінформаційних технології для картування зони ураження та визначення найбільш постраждалих районів, проведення аерокосмічного моніторингу для оцінювання стану і прогнозування розвитку територій;

• співпраця з міжнародними організаціями та екологічними експертами для адаптації сучасних геоінформаційних технологій (ГІС, ДЗЗ і GPS) до реалій України [69];

• участь у міжнародних програмах з відновлення постконфліктних (деокупованих) територій та протидії появі нових депресивних територій, залучення зовнішніх донорів;

• впровадження стандартів і нормативів, що відповідають міжнародним вимогам, для проведення рекультивації порушених земель (штучного відновлення родючості ґрунтів і рослинного покриву після техногенного порушення природи);

• створення нормативно-правового забезпечення для контролю та регулювання процесів відновлення на всіх етапах реалізації регіональної екологічної політики;

• впровадження заходів зі збереження природних цінностей та відновлення біорізноманіття, зокрема через збереження, покращання стану та реінтродукцію зниклих видів, відновлення природних і порушених екосистем [70];

• впровадження в практику господарювання елементів екологічно безпечного, збалансованого використання природних ресурсів з метою не допущення безповоротної втрати частини гено-, демо-, цено- та екофонду, та забезпечити підтримання екорівноваги на території України [71].

• використання природоорієнтованих рішень для відновлення України, таких як: наближене до природи лісівництво; плани управління річковими басейнами; впровадження сталих практик на тлі нищівного впливу війни; ефективна міжсекторна співпраця; нова Зелена політика спрямована на збалансоване використання природних ресурсів тощо [70];

• інноваційні підходи застосування фіторемедіації, біоремедіації та фіторекультивації для очищення техногенно забруднених ґрунтів у сучасних системах землеробства [71];

• управління екологічними ризиками, врахування економічної доцільності та соціальних потреб сприятиме запобіганню катастроф техногенного та екологічного характеру при реалізації екологічної політики [9];

• підвищення рівня громадської обізнаності для збільшення екологічної свідомості та участі у плануванні та реалізації проєктів, що сприятимуть підтримці ініціатив відновлених екосистем [72];

• співробітництво з міжнародними організаціями, науковими установами для розв'язання глобальних екологічних проблем та участь у глобальних ініціативах щодо охорони біологічного різноманіття; охорони транскордонних водотоків і міжнародних озер; зміни клімату; охорони озонового шару; охорони атмосферного повітря; поводження з відходами; оцінки впливу на довкілля [73].

Таким чином, визначення ролі екологічної безпеки як ключового елемента національної безпеки та інтеграція еколого-правових аспектів у загальну стратегію захисту, відновлення та рекультивації територій України, що постраждали від воєнних дій, є важливими завданнями, особливо в контексті поточних викликів. Еколого-правові аспекти національної безпеки в умовах воєнного стану є важливими для збереження довкілля та здоров'я населення, забезпечення сталого місцевого економічного розвитку та відновлення соціальної стабільності після завершення воєнних дій. Розглянуті нормативно-правові акти визначають правила та стандарти для формування нової державної екологічної політики та забезпечення екологічної безпеки в контексті національної безпеки в Україні в умовах воєнного стану; визначають права та обов'язки учасників екологічних відносин та відповідальність за порушення відповідних нормативів у контексті воєнних дій; захищають, попереджають та мінімізують наслідки військових дій на навколишнє середовище.

ВИСНОВКИ

Аналіз свідчить, що розглядати безпеку можна в різних аспектах, таких як національна, економічна, соціальна, інформаційна, екологічна та інші. Кожен із цих видів безпеки має як теоретичне, так і практичне значення. Всі види безпеки розвиваються на основі теоретичних знань, що включають визначення основних понять, аналіз чинників загроз, моделювання сценаріїв розвитку подій та оцінку можливих ризиків. Це також включає розробку систем класифікації загроз, підходів до управління ризиками та створення моделей для прогнозування наслідків.

Теорія безпеки інтегрує знання з різних дисциплін, таких як право, політика, економіка, соціологія, інформаційні технології, екологія тощо. Це дозволяє створити комплексний підхід до забезпечення безпеки. Зокрема, вивчення безпеки включає аналіз політичних, соціальних, економічних та технологічних факторів, що впливають на рівень безпеки. Теоретичні дослідження дозволяють розробляти стратегії та політики, спрямовані на забезпечення різних видів безпеки. Це включає визначення основних напрямків діяльності держави, підприємств та громадськості

у сфері безпеки. В теоретичному аспекті визначаються принципи взаємодії різних суб'єктів (держава, приватний сектор, міжнародні організації) у забезпеченні безпеки. Важливою теоретичною складовою є аналіз та оцінка ризиків, які впливають на безпеку. Це включає ідентифікацію потенційних загроз, їхню класифікацію та визначення можливих наслідків. Ці знання використовуються для розробки методологій, які допомагають приймати обґрунтовані рішення для мінімізації ризиків.

Теоретичне значення дослідження безпеки екологічної, виробничої, економічної, політичної полягає у розвитку та вдосконаленні наукових теорій, концепцій і моделей, які пояснюють механізми впливу людської діяльності на навколишнє середовище. Це включає розробку нових підходів до аналізу ризиків, дослідження стійкості екосистем та розробку методів оцінки впливу на довкілля. Безпека як наукова галузь інтегрує знання з різних дисциплін, таких як екологія, біологія, хімія, географія, економіка, право, соціологія тощо. Це дозволяє створити цілісне уявлення про екологічні процеси та розробити комплексні підходи до їхнього управління. Теоретичне значення включає також розвиток екологічної етики, яка формує моральні принципи та цінності щодо взаємовідносин людини з природою. Це сприяє усвідомленню необхідності збереження біорізноманіття та відповідального ставлення до природних ресурсів. Теоретичні дослідження в сфері екологічної безпеки служать основою для формування національної та міжнародної екологічної політики, яка спрямована на досягнення сталого розвитку та захист навколишнього середовища.

Практичне значення дослідження різних видів безпеки полягає в забезпеченні захисту життєво важливих інтересів як окремих громадян, так і суспільства в цілому. Це включає захист від фізичних загроз, економічної нестабільності, соціальних конфліктів, кіберзагроз та екологічних катастроф. Наприклад, національна безпека захищає державу від зовнішніх загроз, економічна безпека забезпечує стабільний розвиток економіки, а соціальна безпека сприяє підтримці соціальної стабільності.

Практичне значення дослідження включає розробку і впровадження механізмів управління ризиками та кризами. Це дозволяє мінімізувати негативні наслідки можливих загроз та забезпечити стабільність системи в умовах кризи. Це також передбачає розробку планів реагування на надзвичайні ситуації та механізмів швидкого відновлення після кризових подій, полягає у підтримці стабільного функціонування важливих для суспільства систем: економічних, соціальних, інформаційних, екологічних та інших. В практичному контексті безпека стимулює розвиток нових технологій та інновацій, які допомагають підвищити рівень безпеки. Це можуть бути як нові засоби захисту, так і нові методи оцінки та управління ризиками.

Практичне значення різних видів безпеки включає також розвиток міжнародного співробітництва. Глобальні виклики, такі як тероризм, зміни клімату, економічні кризи, вимагають координації зусиль різних держав та міжнародних організацій. Це дозволяє об'єднувати ресурси та досвід для ефективного протистояння загрозам, які не мають національних кордонів. Теоретичне значення дослідження безпеки забезпечує розуміння фундаментальних принципів і механізмів захисту, тоді як практичне значення спрямоване на їхнє впровадження в реальному світі для забезпечення стабільності, розвитку та захисту суспільства.

Практичне значення дослідження безпеки полягає у розробці та впровадженні заходів, які зменшують негативний вплив людської діяльності на навколишнє середовище, попереджають екологічні катастрофи та забезпечують стійкість екосистем. Реалізація принципів безпеки сприяє створенню здорового середовища для життя людей, що включає забезпечення чистої води, повітря, безпечної їжі, а також збереження природних ландшафтів і біорізноманіття.

Практичне значення включає розвиток і впровадження технологій, які забезпечують ефективне використання природних ресурсів, зменшення відходів і забруднення, що дозволяє зберегти ресурси для майбутніх поколінь. Практичне значення екологічної безпеки також полягає у стимулюванні розвитку зеленої економіки, яка базується на використанні екологічно чистих технологій, відновлюваних джерел енергії та циркулярної економіки. Це сприяє створенню нових робочих місць та економічному зростанню при одночасному зменшенні екологічного навантаження.

Практичне значення дослідження полягає у формуванні екологічної свідомості серед населення через освітні програми, громадські кампанії та просвітницьку діяльність. Це дозволяє змінити поведінку людей на більш екологічно відповідальну та сприяє впровадженню екологічно дружніх практик у повсякденному житті. Практичне значення включає також зміцнення міжнародної співпраці у боротьбі зі змінами клімату, забрудненням океанів, зникненням видів тощо, що є необхідним для забезпечення глобальної екологічної безпеки. Практичне впровадження екологічної безпеки допомагає зменшити негативний вплив забруднення довкілля на здоров'я людей, знизити захворюваність і смертність, пов'язані з екологічними проблемами. Це включає заходи щодо зменшення викидів шкідливих речовин у повітря, воду та ґрунт, а також контроль за якістю питної води і продуктів харчування. Впровадження екологічної безпеки на практиці дозволяє раціонально використовувати природні ресурси, зокрема водні, лісові та мінеральні ресурси, що забезпечує їх збереження для майбутніх поколінь. Практичні заходи екологічної безпеки, такі як моніторинг

та контроль за станом навколишнього середовища, допомагають запобігти екологічним катастрофам, таким як розливи нафти, хімічні забруднення та інші аварії. Впровадження екологічної безпеки може мати позитивний економічний ефект, зокрема шляхом зниження витрат на ліквідацію наслідків екологічних катастроф, підвищення ефективності використання ресурсів і зменшення витрат на енергію. Практика впровадження екологічної безпеки сприяє розвитку міжнародного співробітництва в галузі захисту довкілля, зокрема у рамках таких ініціатив, як Паризька кліматична угода та Цілі сталого розвитку ООН. Це дозволяє об'єднувати зусилля різних країн для вирішення глобальних екологічних проблем, таких як зміна клімату, забруднення океанів та збереження біорізноманіття.

Впровадження екологічної, виробничої, економічної, політичної, техногенної безпеки має як теоретичне, так і практичне значення, яке охоплює широкий спектр питань від розвитку наукових концепцій до реалізації конкретних заходів на державному та міжнародному рівнях. Це сприяє не лише захисту навколишнього середовища, але й підвищенню якості життя, зміцненню економічної стабільності та збереженню природних ресурсів для майбутніх поколінь.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ажажа М. А. Зелений екологічний регіон як чинник конкурентоспроможності та сталого розвитку. *"Green Construction" («Зелене будівництво»)* : матеріали ІІ Міжнародної науково-практичної конференції. Київ : Київський національний університет будівництва і архітектури. 2023. С. 291–296. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/17369/1/KNUBA%20Gornostal%2014_04_2023.pdf

2. Ажажа М. А., Нікітенко В. О., Венгер О. М., Фурсін О. О. Зелені технології та стратегії сталого розвитку як чинники забезпечення безпеки громадян та збереження навколишнього середовища. *"Green Construction" («Зелене будівництво»)* : матеріали ІІІ Міжнародної науково-практичної конференції . Київ : Київський національний університет будівництва і архітектури. 2024. С. 11–16.

3. Бугайчук О. В. Машинний інтелект, штучне і глибинне навчання як чинники розвитку діджиталізованого менеджменту. *Економіко-правові дискусії* : матеріали ІІІ Міжнародної науково-практичної Інтернет-конференції студентів, аспірантів та науковців, 30 квітня 2022 р. Кропивницький : ЛА НАУ, 2022. С. 96–97.

4. Венгер Ольга. Філософія ризик-менеджменту у контексті глобальних викликів. anagerial, social and technological innovations – the basis of the public good = Vadybinės, socialinės ir technologinės inovacijos – visuomenės gerovės pagrindas : tarptautinės mokslinės – praktinės konferencijos tezių rinkinys. *Lithuania Marijampolė, Marijmpolės kolegija*. 2023. С. 82–83.

5. Воронкова В. Г., Череп А. В,, Нікітенко В. О., Череп О. Г. Політика національної безпеки як чинник забезпечення стабільності та захисту інтересів держави. Contemporary ukrainian science: theoretical and practical achievements : collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board: S. Tabachnikov. Sherman Oaks, California : GS Publishing Services, 2024. С. 40–55. DOI : 10.51587/9798-9866-95952-2024-018

6. Воронкова В. Г. Формування концепції стратегії кібербезпеки в умовах глобалізації: економічні засади. Scientific trends: modern challenges. Volume 1 : collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California : GS Publishing Services, 2021. С. 46–60.

7. Воронкова В. Г. Напрями захисту суспільства та особистості у протидії кібезлочинності. *Аспекти публоічного управління* : матеріали конференції «Публічне управління у цифровому суспільстві» 25 червня 2020 року. 2020. Т. 8. Спеціальний випуск 1. Дніпро : Дніпропетровський регіональний інститут державного управління Національної академії державного управління. С. 25–27. URL: https://aspects.org.ua/index.php/journal/article/view/750

8. Воронкова В. Г., Нікітенко В. О. Концепція інформаційного забезпечення менеджменту в організації. *Теоретичні та практичні засади розвитку економіки, обліку, фінансів, менеджменту та права* : матеріали Всеукраїнської науково-практичної конференції 23–24 листопада 2021 року. Запорізький національний університет. Запоріжжя : ЗНУ, 2021. С. 47–48.

9. Воронкова В. Г., Нікітенко В. О., Андрюкайтене Регіна. Культура безпеки як складна соціально-економічна і морально-етична проблема. *Стратегічні пріоритети розвитку підприємництва, торгівлі та біржової діяльності* : матеріали IV Міжнародної науково-практичної конференції, 10–11 травня 2023 року / за заг. редак. проф. Ткаченко А. М. Запоріжжя : НУ «Запорізька політехніка», 2023. С. 57–61.

10. Воронкова В. Г., Крупа А. Г. Цифрова безпека як чинник захисту людини, організації, суспільства. *Актуальні питання сталого науково-технічного та соціально-економічного розвитку регіонів України* : матеріали III Всеукраїнської науково-практичної конференції за участю молодих науковців, 17–20 жовтня 2023 року. Запоріжжя : ЗНУ, 2023. С. 548–549. URL: https://www.znu.edu.ua/ii_znu/nauka/conf6/zbirnyk_23.pdfhttps://www.znu.edu.ua/ii_znu/nauka/conf6/zbirnyk_23.pdfhttp://eir.zntu.edu.ua/bitstream/123456789/10033/1/Strategic_priorities.pdf

11. Воронкова В. Г., Крупа А. Г. Цифрова безпека як чинник захисту людини, організації, суспільства. *Актуальні питання сталого науково-технічного та соціально-економічного розвитку регіонів України* : матеріали III Всеукраїнської науково-практичної конференції за участю молодих науковців, 17–20 жовтня 2023 року. Запоріжжя : ЗНУ, 2023. С. 548–549. URL: https://www.znu.edu.ua/ii_znu/nauka/conf6/zbirnyk_23.pdf

12. Valentina, Voronkova, Yuriy, Kaganov, Natalia, Metelenko. Formation of digital society and digital man values in the globalization conditions and Industry 4.0. *Humanities studies* : Collection of Scientific Papers / Ed. V. Voronkova. Zaporizhzhia : Publishing house “Helvetica”. Запоріжжя : Видавничий дім «Гельветика», 2022. Вип. 11 (88). С. 16–25. URL: http://humstudies.com.ua/article/view/261854/258244

Воронкова В. Г., Ажажа М. А., Нікітенко В. Цивілізація, залежна від викопного палива. *Еко Форум – 2021* : збірка тез доповідей V спеціалізованого міжнародного Запорізького екологічного форуму, 14–16 вересня 2021 р. / Запорізька міська рада, Запорізька торгово-промислова палата. Запоріжжя : Запорізька торгово-промислова палата, 2021. С. 80–81. URL: https://ziif.in.ua/wp-content/uploads/2021/09/tezysy-21_sajt.pdf

13. Voronkova Valentyna, Cherep Alla, Nikitenko Vitalina, Cherep Olexandr. Artificial intelligence and its attributes: conditions for improving functionality and interaction wi ograph / Compiled by V. Shpak; Chairman of the Editorial Board: S. Tabachnikov. Sherman Oaks California : GS Publishing Services, 2023. С. 39–55. Available at: DOI : 10.51587/9798-9866-95969-2023-06

14. Воронкова В. Г., Нікітенко В. О. Концепція інформаційного забезпечення менеджменту в організації. *Теоретичні та практичні засади розвитку економіки, обліку, фінансів, менеджменту та права* : матеріали Всеукраїнської науково-практичної конференції 23–24 листопада 2021 року. Запорізький національний університет. Запоріжжя : ЗНУ, 2021. С. 47–48.

15. Воронкова Валентина, Нікітенко Віталіна. «Суспільство ризику» як назва сучасної епохи. *Соціальне прогнозування та проєктування майбутнього: перемога, мир та відновлення у післявоєнній Україні* : матеріали XIII Міжнародної наукової конференції (28 квітня 2023 року, м. Запоріжжя) / І. О. Кудінов (гол. ред.), М. А. Лепський (наук. ред.) ; ред. кол.: Т. Ф. Бірюкова, Н. В. Лепська, Т. І. Бутченко, В. О. Скворець, Є. Г. Цокур. Запоріжжя : ЦНСД, 2023. С. 28–32. URL: https://socforecast.org.ua/wp-content/uploads/socforecast2023.pdf

16. Воронкова В. Г., Череп А. В,, Нікітенко В. О., Череп О. Г. Політика національної безпеки як чинник забезпечення стабільності та захисту інтересів держави. Contemporary ukrainian science: theoretical and practical achievements : collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board: S. Tabachnikov. Sherman Oaks, California : GS Publishing Services, 2024. С. 40–55.

17. Воронкова В. Г., Нікітенко В. О., Кивлюк О. П., Бєлоконь К. В., Карпенко Г. В. Філософія штучного інтелекту (ШІ) як міждисциплінарна галузь знань з філософії, комп'ютерних наук, техногенної безпеки, права та психології. *Business culture in the conditions of socio-cultural transformation of society* : the 29th International scientific and practical conference (July 23–26, 2024) Lyon, France. International Science Group. 2024. С. 165–174. URL: https://isg-konf.com/business-culture-in-the-conditions-of-socio-cultural-transformation-of-society/

18. Воронкова В. Г., Метеленко Н. Г., Нікітенко В. О. Система мережевої безпеки як чинник забезпечення цілісності кіберпростору. *Perspectives of contemporary science: theory and practice* : VII Міжнародна науково-практична конференція, 19–21.08.2024 року. Львів, 2024.

19. Воронкова Валентина. Штучний інтелект (ШІ) як каталізатор трансформації бізнесу, підприємств, організацій. *Theory and Practice: Problems and Prospects* : International Scientific-Practical Conference: Book of Abstracts, 14th–15th of May, 2024 Virtual Conference. С. 38. URL: http://dspace.lsu.lt/handle/123456789/120

20. Klopov Ivan, Shapurov Olexandr, Voronkova Valentyna, Nikitenko Vitalina, Oleksenko Roman, Khavina Irina, Chebakova Yuliia. Digital Transformation

of Education Based on Artificial Intelligence. *TEM Journal*. Vol. 12, Is. 4. P. 2625–2634. ISSN 2217-8309. DOI: 10.18421/TEM124-74, November 2023. URL: https://www.temjournal.com/content/124/TEMJournalNovember2023_2625_2634.pdf

21. Крупа Андрій. Штучний інтелект як чинник розвитку цифрової економіки. Managerial, social and technological innovations – the basis of the public good = Vadybinės, socialinės ir technologinės inovacijos – visuomenės gerovės pagrindas : tarptautinės mokslinės – praktinės konferencijos tezių rinkinys. Lithuania Marijampolė, Marijmpolės kolegija, 2023.С. 41–42. URL: https://marko.lt/moksline-veikla/; URL: https://marko.lt/wp-content/uploads/2023/09/Tesis-book_Marijampole_2023_pdf.pdf

22. Мар'єнко В. Ю. Інформаційне забезпечення менеджменту в організаціях як складних системах в умовах цифровізації. Modern scientific strategies of development : collective monograph / Compiled by V. Shpak ; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California : GS Publishing Services, 2022. P. 62–81. DOI: 10.51587/9781-7364-13395-2022-008-62-8

23. Мар'єнко В. Ю. Інформаційна безпека як умова вирішення глобальних проблем міжнародного простору. С. 120–125. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. С. 17–22.

24. Marienko, Victoria, Voronkova, Valentyna, Nikitenko, Vitalina. Informatisation of the digital economy as the main trend of exponential development. *Baltic Journal of Economic Studies.* Latvia : "Baltija Publishing". 2023. Vol. 9. № 4 (2023). P. 178–183.

25. Мар'єнко В. Ю. Вплив інформаційно-комунікаційних технологій (ІКТ) на розвиток суспільства, людини, техніки: соціально-філософський аналіз. *Освітній дискурс: збірник наукових праць* / голов. ред. О. П. Кивлюк. Київ : ТОВ «Науково-інформаційне агентство «Наука-технології-інформація». 2023. Вип. 47 (12) С. 61–72. URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/44509/Marienko-61-72.pdf?sequence=1&isAllowed=y

26. Мар'єнко В. Ю. Безпека даних в епоху великих даних як стратегічний ресурс країни. *Стратегічні пріоритети розвитку підприємництва, торгівлі та біржової діяльності* : матеріали IV Міжнародної науково-практичної конференції, 10–11 травня 2023 року / за заг. ред. проф. А. М. Ткаченко. Запоріжжя : НУ «Запорізька політехніка», 2023. С. 76–80. URL: http://eir.zntu.edu.ua/bitstream/123456789/10033/1/Strategic_priorities.pdf

27. Метеленко Наталя, Воронкова Валентина. Концепція глобальних ризиків та їх вплив на світову економіку та політику. Managerial, social and technological innovations – the basis of the public good = Vadybinės, socialinės ir technologinės inovacijos – visuomenės gerovės pagrindas : tarptautinės mokslinės – praktinės konferencijos tezių rinkinys. Lithuania Marijampolė, Marijmpolės kolegija, 2023. С. 54–56.

28. Метеленко Н. Г., Андрюкайтене Регіна. ІКТ нового покоління як чинник розвитку інноваційної економіки цифрового століття. *Економіко-правові та соціально-технічні напрями еволюції цифрового суспільства* : матеріали міжнародної науково-практичної конференції: у 2 т. Т. 2. Дніпро : Університет митної справи та фінансів, 2022. С. 449–451. URL: https://drive.google.com/file/d/1ESCY5IAFSK1AhXTrUrSLpKwD4I80-nr1/view

29. Metelenko N., Nikitenko V., Meniailo, V. (2024). Development of the smart economy as the main source of competitiveness and sustainable development. (Розвиток смарт-економіки як головне джерело конкурентоспроможності і стійкого розвитку). *Baltic Journal of Economic Studies.* № 10 (2). P. 187–195. DOI: https://doi.org/10.30525/2256-0742/2024-10-2-187-195. URL: http://baltijapublishing.lv/index.php/issue/article/view/2427

30. Нікітенко В. О., Воронкова В. Г., Череп А. В. Концепція культури безпеки як чинника соціальної відповідальності (СВ) організацій. *Стратегічні пріоритети розвитку підприємництва, торгівлі та біржової діяльності* : матеріали IV Міжнародної науково-практичної конференції, 10–11 травня 2023 року / за заг. редак. проф. А. М. Ткаченко. Запоріжжя : НУ «Запорізька політехніка», 2023. 372 с. С. 80–84. URL: http://eir.zntu.edu.ua/bitstream/123456789/10033/1/Strategic_priorities.pd

31. Нікітенко В. О., Воронкова В. Г., Череп А. В. Концепція культури безпеки як чинника соціальної відповідальності (СВ) організацій. *Стратегічні пріоритети розвитку підприємництва, торгівлі та біржової діяльності* : матеріали IV Міжнародної науково-практичної конференції, 10–11 травня 2023 року / за заг. редак. проф. А. М. Ткаченко. Запоріжжя : НУ «Запорізька політехніка», 2023. С. 80–84.

32. Нікітенко В. О., Кивлюк О. П. Системне та дата-аналітичне мислення як стратегічні ресурси сучасних організацій. *Системний аналіз в управлінні: міжгалузеві дослідження* : матеріали IV Всеукраїнської науково-практичної конференції за міжнародної участі 26–27 травня 2022 року / Національний педагогічний університет імені М. П. Драгоманова. Київ : Ореол-Сервіс, 2022. С. 77–80. URL: https://kuei.fmon.npu.edu.ua/nauka/naukovi-zbirnyky

33. Про національну безпеку України : Закон України № 2469-VIII від 21 червня 2018 р. *Відомості Верховної Ради України*. 2018. № 31. С. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

34. Промисловий менеджмент: теорія і практика: колективна монографія / за ред. д.філос.н., проф. В. Г. Воронкової, д.е.н., проф. Н. Г. Метеленко. Запоріжжя : Запорізький національний університет. 2020. 338 с. URL: https://dspace.znu.edu.ua/jspui/handle/12345/3282

35. Промисловий потенціал складних соціально-економічних систем цифрового суспільства: макро-, мезо- та мікрорівень ; колективна моногрфія / за ред. д.філософ.н., проф. В. Г. Воронкової, д.е.н., проф. Н. Г. Метеленко. Запоріжжя : Видавний дім «Гельветика». 2022. 480 с. URL: https://catalog.liha-pres.eu/index.php/liha-pres/catalog/book/154

36. Sliusar Mykyta. Stablishment and development of the network platform model in China and its impact on the formation of the digital economy. *Humanities studies: Collection of Scientific Papers. Zaporizhzhia: Publishing house "Helvetica"*. 2023. № 14 (91). P. 165–175. URL: http://humstudies.com.ua/article/view/277867/272615

37. Слюсар Никита. Місце і роль цифрових платформ в умовах розвитку Четвертої промислової революції. The 8th International scientific and practical conference "International scientific innovations in human life" (February 16–18, 2022) Cognum Publishing House, Manchester, United Kingdom. 2022. 687 p. С. 610–620. URL: https://sci-conf.com.ua/viii-mezhdunarodnaya-nauchno-prakticheskaya-kon

ferentsiya-international-scientific-innovations-in-human-life-16-18-fevralya-2022-goda-manchester-velikobritaniya-arhiv/ї

38. Управління сталим розвитком промислового підприємства: теорія і практика : колективна монографія / за ред. д.філософ.н., проф. В. Г. Воронкової, д.е.н., проф. Н. Г. Метеленко ; МОН України, ЗНУ ІННІ. Запоріжжя : Видавничий дім «Гельветика», 2021. 586 с.

39. Цифрова трансформація промислового менеджменту: теорія і практика : монографія / за ред. д.філософ.н., проф. В. Г. Воронкової, д.е.н., проф. Н. Г. Метеленко. Львів – Торунь : Liha-Pres, 2023. 816 с. URL: https://dspace.znu.edu.ua/jspui/handle/12345/13677

40. Череп А. В., Воронкова В. Г., Нікітенко В. О., Череп О. Г. Стратегії протидії кіберзагрозам як фактор забезпечення стійкості національної безпеки у цифрову епоху. *Modern science: multidisciplinary discourses* : collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman, Oaks, California : GS Publishing Services, 2024. С. 56–74. URL: https://www.eo.kiev.ua/ua/content/148/

40. Череп А. В., Воронкова В. Г. Європейські практики діджиталізації як інструмент забезпечення соціально-економічної безпеки. *Менеджмент та маркетинг як фактори розвитку бізнесу* : матеріали ІІ Міжнародної науково-практичної конференції 17–19 квітня 2024 р. Електронне видання у 2 т. / відп. ред. та упоряд. В. В. Храпкіна, К. В. Пічик. Київ : Видавничий дім «Києво-Могилянська академія», 2024. Т.2. С. 396–400. URL: https://elartu.tntu.edu.ua/bitstream/lib/44750/1/TEZY.pdf

41. Алла Череп, Валентина Воронкова, Регіна Андрюкайтене, Максим Денисенко. Соціально-економічна безпека у контексті міжнародного економічного клімату задля забезпечення конкурентоспроможності економіки. *Acta Academia Beregsasiensis. Econom*ics. Вип. 3 (2023). Vol. 3 (2023). С. 172–179. URL: https://aab-economics.kmf.uz.ua/aabe/article/view/87/84

42. Череп А. В., Воронкова В. Г. Соціально-економічна безпека як чинник забезпечення конкурентоспроможності економіки. *Методологія сучасних наукових досліджень* : збірник наукових праць за результатами XIX Міжнародної науково-практичної конференції 23–24 лютого 2023 року. Харків : Вид-во Харківського національного педагогічного університету імені Г. С. Сковороди, 2023. С. 238–241.

43. Череп А. В., Нікітенко В. О., Воронкова В. Г. Становлення і розвиток концепції людської безпеки як чинник людського розвитку та досягнення прогресу. *Соціально-гуманітарні виміри правової держави* : матеріали Міжнародної науково-практичної конференції (м. Дніпро, 14 квітня 2023 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2023. С. 103–107.

44. Cherep A. V., Voronkova V. H., Cherep O. Humanocracy as a factor of improving human resources management in organization. *Humanities studies : Collection of Scientific Papers. Zaporizhzhia : Publishing house "Helvetica*", 2022. Вип. 10 (87). С. 134–141. URL: http://humstudies.com.ua/article/view/254724

45. Добробог Людмила. Екологічна безпека України в умовах воєнного стану. Секція: міжнародна та національна безпека: теоретичні та прикладні аспекти. *Матеріали VII Міжнародної науково-практичної конференції* (ДДУВС, 17.03.2023). URL: https://er.dduvs.in.ua/bitstream/123456789/11387/1/87.pdf

46. Семерня О. М. Екологічна безпека в умовах воєнного стану / Любинський О. І., Федорчук І. В., Рудницька Ж. О., Семерня А. О. *Науково-практичний журнал «Екологічні науки».* 2022. № 2 (41). URL: http://ecoj.dea.kiev.ua/archives/2022/2/11.pdf

47. Антонюк У. В. Правові аспекти доступу до екологічної інформації в Україні в умовах воєнного стану. *Київський часопис права.* 2023. № 1. С. 136–141. URL: https://doi.org/10.32782/klj/2023.1.20

48. Конституція України. URL: http://surl.li/gdyl

49. Ажажа М. А. Правові засади екологічного аспекту національної безпеки України в умовах воєнного стану. *Публічне управління у сфері цивільного захисту: освіта, наука, практика* : збірник матеріалів міжнародної науковопрактичної інтернет-конференції, м. Харків, 29 березня 2024 р. / за заг. ред. С. М. Домбровської. Харків : НУЦЗУ, 2024. 253 с. С. 49–51. URL: https://nuczu.edu.ua/images/topmenu/science/konferentsii/2024/ZbPUA2024.pdf

50. Закон України «Про охорону навколишнього природного середовища». URL: https://zakon.rada.gov.ua/laws/show/1264-12#Text

51. Закон України «Про правовий режим воєнного стану». URL: https://zakon.rada.gov.ua/laws/show/389-19#Text

52. Закон України «Про національну безпеку України». URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

53. Закон України «Основні засади (стратегія) державної екологічної політики України на період до 2030 року». URL: https://zakon.rada.gov.ua/laws/show/2697-19#Text

54. Закон України «Про охорону атмосферного повітря». URL: https://zakon.rada.gov.ua/laws/show/2707-12#Text

55. Закон України «Про управління відходами». URL: https://zakon.rada.gov.ua/laws/show/2320-20#Text

56. Закон України «Про внесення змін до деяких законодавчих актів України щодо державної системи моніторингу довкілля, інформації про стан довкілля (екологічної інформації) та інформаційного забезпечення управління у сфері довкілля». URL: https://zakon.rada.gov.ua/laws/show/2973-20#Text

57. Кодекс цивільного захисту України. URL: https://zakon.rada.gov.ua/laws/show/5403-17

58. Водний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/213/95-%D0%B2%D1%80#Text

59. Женевська конвенція про захист цивільного населення під час війни. URL: https://zakon.rada.gov.ua/laws/show/995_154#Text

60. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1997 року. URL: https://zakon.rada.gov.ua/laws/show/995_199

61. Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD). URL: https://disarmament.unoda.org/enmod/

62. Конвенція про заборону або обмеження застосування конкретних видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень або мають невибіркову дію. URL: https://zakon.rada.gov.ua/laws/show/995_266#Text

63. Рамкова конвенція Організації Об'єднаних Націй про зміну клімату. https://zakon.rada.gov.ua/laws/show/995_044#Text

64. Кіотський протокол до Рамкової конвенції ООН. URL: https://zakon.rada.gov.ua/laws/show/995_801#Text

65. Ажажа М. А., Нікітенко В. О., Венгер О. М., Фурсін О. О. Зелені технології та стратегії сталого розвитку як чинники забезпечення безпеки громадян та збереження навколишнього середовища. Матеріали III Міжнародної науково-практичної конференції "Green Construction" («Зелене будівництво»). Київ : Київський національний університет будівництва і архітектури. 2024, 443 с. С. 11–15. URL: https://www.knuba.edu.ua/wp-content/uploads/2024/05/zbirnyk_gotovyj-4.pdf

66. Екологічний моніторинг довкілля. Сайт Міністерства захисту довкілля та природних ресурсів України. URL: https://mepr.gov.ua/pro-nas/kerivnytstvo/

67. Воронкова В. Г., Ажажа М. А., Нікітенко В. Цивілізація, залежна від викопного палива. Еко Форум–2021 : збірка тез доповідей V спеціалізованого міжнародного Запорізького екологічного форуму, 14–16 вересня 2021 р. / Запорізька міська рада, Запорізька торгово-промислова палата. Запоріжжя : Запорізька торгово-промислова палата, 2021. С. 80–81.

68. Про Концепцію збереження біологічного різноманіття України. URL: https://zakon.rada.gov.ua/laws/show/439-97-%D0%BF#Text

69. Концепція Загальнодержавної програми збереження біорізноманіття на 2005–2025 роки. URL: https://www.kmu.gov.ua/npas/9110364

70. Рішення, натхненні природою: на COP28 обговорили роль природоорієнтованих рішень для відновлення України. URL: https://mepr.gov.ua/rishennya-nathnenni-pryrodoyu-na-sor28-obgovoryly-rol-pryrodooriyentovanyh-rishen-dlya-vidnovlennya-ukrayiny/

71. Інноваційні підходи до фіторемедіації та фіторекультивації у сучасних системах землеробства. Монографія / Я. Г. Цицюра, Ю. М. Шкатула, Т. А. Забарна, Л. В. Пелех. Вінниця : ТОВ «Друк», 2022. 1200 с. URL: http://repository.vsau.org/getfile.php/31038.pdf

72. Зелене відновлення України: 2023 керівні принципи та інструменти для тих, хто ухвалює рішення. URL: https://www.undp.org/sites/g/files/zskgke326/files/2024-04/undp-ua-green-recovery-ukr.pdf

73. Співробітництво з міжнародними організаціями. *Сайт Міністерства захисту довкілля та природних ресурсів України.* URL: https://mepr.gov.ua/diyalnist/mizhnarodna-diyalnist/spivrobitnytstvo-z-mizhnarodnymy-organizatsiyamy/