РОЗДІЛ 1. УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ В УМОВАХ ЗАГРОЗ ТА КРИЗ

Горбаченко Станіслав Анатолійович
д.е.н., професор, завідувач кафедри кібербезпеки,
Національний університет «Одеська юридична академія»

Саврацький Олександр Олександрович
аспірант кафедри кібербезпеки,
Національний університет «Одеська юридична академія»

УПРАВЛІНСЬКІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

DOI https://doi.org/10.36059/978-966-397-537-5-1

В умовах сучасних геополітичних викликів жодна країна не в змозі забезпечити повний та абсолютний захист власної інфраструктури від впливу зовнішніх чинників. Відтак, єдиний альтернативний варіант полягає у зосередженні основних ресурсів на захисті критично важливих об'єктів. В цьому сенсі термін «критичність» вказує на вірогідність появи небезпеки чи певних скрутних обставин, які, в майбутньому можуть призвести до кризи або інших негативних наслідків.

На державному рівні саме критична інфраструктура є тим фундаментом, на якому тримається стабільність забезпечення основних послуг та функцій, необхідних для нормального функціонування суспільства. Отже кожна країна прагне сформувати власні унікальні стратегії, підходи та інструменти для забезпечення безпеки об'єктів критичної інфраструктури. При цьому орієнтація йде, насамперед, на ті специфічні загрози та вразливості, які генерує кіберсередовище. Особливо загрози кіберсередовища є актуальними для Україні, де з початком повномасштабної агресії спостерігається різке зростання і кількості цілеспрямованих кібератак на критичну інфраструктуру: енергетичну, транспортну, фінансову, урядову тощо.

В контексті посилення кіберзагроз забезпечення надійності, стійкості та безперебійності функціонування критичної інфраструктури є не лише результатом пошуку та використання відповідних технічних безпекових рішень. Одночасно із цим актуалізуються питання законодавчої підтримки, профільних наукових досліджень, впровадження управлінських інновацій, роботи з персоналом підприємств, що відносяться до критичної інфраструктури, організації міжнародної співпраці в сфері кібербезпеки тощо. З огляду на вищезазначене ефективне управління критичною інфраструктурою є неможливим без залучення та координації різних зацікавлених сторін, включаючи органи державної та місцевої влади, бізнес-структури та громадянське суспільство.

Однак на практиці існуючі управлінські підходи все ще недостатньо адаптовані до протидії кіберзагрозам. Зокрема, багато об'єктів критичної інфраструктури не мають ані регламентованих процедур, ані чіткої відповідальності за кіберзахист на рівні керівництва. Отже проблема збільшення ефективності кіберзахисту виходить за межі технічних змін і потребує, у тому числі, оновлення управлінських підходів.

Питання організації кіберзахисту критичної інфраструктури, в тих чи інших аспектах, виступали об'єктом досліджень значної кількості науковців, серед яких Д. Бірюков, І. Діордіца, О. Довгань, Д. Кобилкін, С. Кондратов, О. Суходоля, В. Ящук та інші. Однак, незважаючи на, значний науковий доробок управлінська проблема побудови ефективного кіберзахисту все ще не вирішена. Адже кіберзагрози постійно трансформуються та еволюціонують, стають все більш складними та витонченими. Як приклад можна навести використання штучного інтелекту при кібератаках, що, у свою чергу, вимагає системних та комплексних змін всієї управлінської ланки, особливо у сегменті критичної інфраструктури, який виступає головним об'єктом для кібератак. Тому дослідження управлінської складової кіберзахисту критичної інфраструктури України не втрачають власної актуальності.

Мета дослідження полягає у виявленні можливостей для збільшення ефективності захисту об'єктів критичної інфраструктури від кіберзагроз за рахунок організаційно-управлінських підходів.

Поставлена мета передбачає вирішення наступних завдань:

– проаналізувати сучасні кіберзагрози, що становлять небезпеку для об'єктів критичної інфраструктури;

– оцінити рівень захищеності об'єктів критичної інфраструктури на основі наявних нормативних, організаційних та технічних рішень;

– дослідити існуючі організаційно-управлінські підходи до забезпечення кібербезпеки критичної інфраструктури;

– визначити ключові проблеми в управлінні кіберзахистом на рівні об'єктів критичної інфраструктури;

– обґрунтувати доцільність впровадження менеджменту кібербезпеки в діяльність об'єктів критичної інфраструктури.

Об'єкт дослідження – управлінські процеси забезпечення кіберзахисту об'єктів критичної інфраструктури.

Предметом дослідження виступають управлінські підходи, методи та інструменти підвищення ефективності кіберзахисту об'єктів критичної інфраструктури України.

Критична інфраструктура може розглядатися як сукупність об'єктів, які є стратегічно важливими для економіки та національної безпеки, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [1]. Тобто мова йде про об'єкти, які є настільки важливими для функціонування держави, що їхнє знищення, критичне пошкодження або, навіть, тимчасове припинення функціонування можуть мати значний (а, в деяких випадках, й невідворотній) вплив на національну безпеку, економічний потенціал країни, конкурентоспроможність окремих галузей, якість життя населення тощо.

З функціонального погляду критична інфраструктура розглядається як сукупність об'єктів незалежно від форми власності, що реалізують функції, виробляють товари (послуги), які є життєво необхідними для людей і діяльності країни та порушення яких призведе до дестабілізації суспільних відносин [2].

З точки зору прив'язки до економічної діяльності критичну інфраструктуру також можна розглядати як сукупність об'єктів, систем, мереж, послуг, які є стратегічно важливими для економіки та безпеки країни, суспільства, населення і пошкодження, знищення або порушення діяльності яких може завдати шкоди життєво важливим інтересам України [3].

За ресурсним підходом критичною інфраструктурою України є системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призводять до найсерйозніших негативних наслідків для життя суспільства та соціально-економічного розвитку країн та національної безпеки [4].

Враховуючи сучасні тренди цифрової трансформації, що відбуваються у сучасному суспільстві в деяких визначеннях фігурує й інформаційна (нематеріальна) складова критичної інфраструктури. В цьому випадку, критичну інфраструктуру визначають як систему надзвичайно важливих матеріальних та нематеріальних об'єктів національної інфраструктури (а також їхню власність та результати діяльності), що забезпечують її стале функціонування, руйнація або пошкодження яких (наявними загрозами) може призвести до людських жертв і значних матеріальних збитків із найсерйознішими негативними наслідками для життєдіяльності суспільства, соціально-економічного розвитку країни та національної безпеки [5].

Виходячи з галузевого підходу критична інфраструктура – системний комплекс стратегічних матеріальних та інформаційних об'єктів виробничої, невиробничої, соціальної сфери, а також окремих складових частин цього комплексу, у тому числі ключових ресурсних, покликаних забезпечувати повноцінний життєвий цикл, безпеку, охорону здоров'я, добробут людини, сталий розвиток суспільства й економіки держави, підтримання її суверенітету з огляду на те, що зловмисне втручання у функціонування, а також пошкодження, руйнація або виведення з ладу системи або її елементів внаслідок диверсій, техногенних чи природних катастроф спроможне призвести до тяжких наслідків: жертв чи поневірянь, шкоди національним інтересам, знецінення надбань людини і держави [6].

Об'єкти критичної інфраструктури відзначаються значною різноманітністю за своїми характеристиками. По-перше, до критичної інфраструктури відносять як матеріальні (фізичні), так і нематеріальні (інформаційно-комунікаційні) компоненти. До фізичних об'єктів можна віднести електростанції, системи централізованого водопостачання, транспортні вузли, аеропорти, залізничні станції, мости та інші інженерні споруди, від яких залежить нормальне функціонування суспільства. Водночас інформаційно-комунікаційна інфраструктура

охоплює телекомунікаційні мережі, центри обробки даних, хмарні сервіси, системи зв'язку та управління, які забезпечують безперебійне передавання та збереження критично важливої інформації.

По-друге, зазначені об'єкти можуть належати до різних форм власності. Вони бувають державними (наприклад, об'єкти енергетичного сектору, морські та річкові порти, оборонні підприємства), муніципальними (заклади охорони здоров'я, комунальні підприємства, системи громадського транспорту), а також приватними (мобільні оператори, провайдери інтернету, логістичні структури, банківські установи). Вказана ситуація зумовлює потребу у координації між різними власниками та органами державної влади для забезпечення надійного функціонування інфраструктури в умовах криз чи надзвичайних ситуацій.

По-третє, діяльність таких об'єктів може здійснюватися на різних економічних засадах. Частина з них функціонує як неприбуткові установи (наприклад, системи очищення води, санітарно-епідеміологічні служби), інші мають змішану модель фінансування та умовно-прибутковий характер (наприклад, державні лікарні, освітні заклади). Нарешті, значна кількість об'єктів критичної інфраструктури працює як комерційні структури з чітко вираженою ринковою орієнтацією: банки, підприємства агропромислового комплексу, великі енергетичні підприємства тощо.

Тобто, критична інфраструктура охоплює за статусом широкий спектр об'єктів, що відрізняються за своєю природою, формою власності та економічною моделлю. З іншого боку можна виділити декілька ключових аспектів, що є спільними для переважної більшості об'єктів критичної інфраструктури (табл. 1).

Таким чином, незважаючи на внутрішню неоднорідність, основне призначення усіх об'єктів критичної інфраструктури полягає у створенні умов для реалізації базових потреб людини та найважливіших функцій держави. Відтак ієрархія об'єктів критичної інфраструктури ґрунтується, насамперед, на показнику критичності, який визначає ступінь (відносний рівень) важливості об'єкта і його вплив на суспільство. Згідно показника критичності до першої категорії відносяться об'єкти, що мають високу важливість для держави в цілому і здатні суттєво впливати на інші об'єкти критичної інфраструктури.

Таблиця 1 – Характерні риси об'єктів критичної інфраструктури [7]

№	Характеристика	Опис
1	Забезпечують надання надважливих послуг.	Надають послуги, від яких критично залежить не тільки економіка, а й усе суспільство: транспорт, енергетика, водопостачання, охорона здоров'я тощо.
2	Значна роль в національній безпеці.	Перебої у функціонуванні об'єктів критичної інфраструктури можуть мати серйозні наслідки для обороноздатності країни. Одночасно, є першими цілями для фізичних атак в умовах військових конфліктів.
3	Ризики кіберсередовища.	Є головною мішенню для кібератак, особливо в умовах військових конфліктів.
4	Активне державне втручання в діяльність.	Держава формує перелік об'єктів критичної інфраструктури, встановлює та, за необхідністю, змінює правила та норми для їхнього функціонування з метою підтримки надійності та безперебійності.
5	Залежність від міжнародної співпраці.	Забезпечення захисту об'єктів критичної інфраструктури потребує міжнародної координації та співпраці, особливо в ситуації, коли вплив критичної інфраструктура виходить за межі національних кордонів (транспорт, енергетика).

Якщо їхня робота буде порушена, виникне кризова ситуація державного значення. Друга категорія включає об'єкти, що є життєво важливими, а припинення чи порушення їх роботи спричинить кризову ситуацію регіонального значення. Третя категорія – важливі об'єкти, порушення чи припинення роботи яких спричинить кризову ситуацію місцевого значення. І, нарешті, четверта категорія складається з об'єктів, порушення чи припинення роботи яких спричинить кризову ситуацію локального значення [8].

В науковій літературі існує багато підходів до ідентифікації об'єктів критичної інфраструктури, зокрема: функціональний, системний, ризик-орієнтований, територіальний, економічний та нормативний, інтегрований підходи (рис. 1). Їх умовно можна поділити на дві основні групи – ті, що орієнтовані на характеристики об'єктів, та ті, що орієнтовані на аналіз ризиків і управління ними.

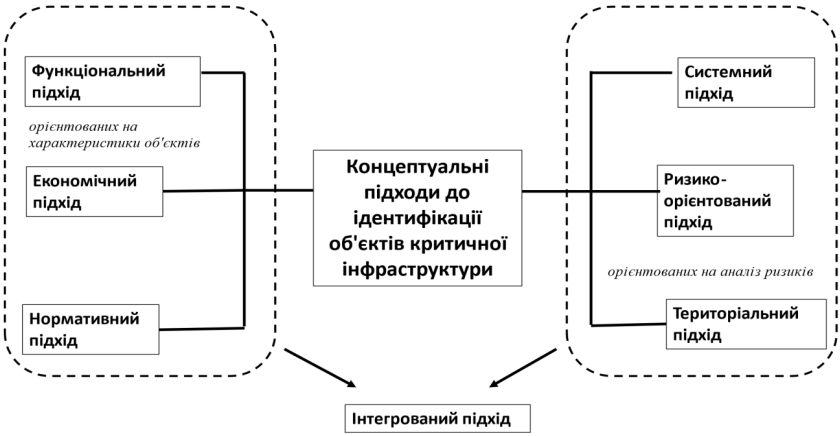

Рисунок 1 – Концептуальні підходи до ідентифікації об’єктів критичної інфраструктури

Обидві категорії підходів до управління критичною інфраструктурою – орієнтовані на характеристики об’єктів та орієнтовані на ризики – формують власні системи методів, інструментів та процедур, які застосовуються в залежності від мети аналізу та управлінських завдань. Підходи, що фокусуються на внутрішніх характеристиках об’єктів (структурі, функціональності, масштабах, забезпеченості ресурсами тощо), зазвичай використовуються при стратегічному плануванні, модернізації інфраструктури, розподілі фінансових та матеріальних ресурсів, а також для оцінки потужностей і можливостей реагування на підвищене навантаження.

Натомість підходи, що базуються на аналізі ризиків, є ключовими для забезпечення надійності та стійкості функціонування інфраструктурних об’єктів у надзвичайних умовах. Вони лежать в основі створення системи управління кризовими ситуаціями, розробки планів реагування на кіберінциденти, сценарного моделювання загроз, а також впровадження превентивних заходів для зниження уразливості інфраструктури.

Розмежування між цими підходами визначається передусім їхніми цільовими орієнтирами та застосовуваними методами аналізу. У кожному конкретному випадку вибір того чи іншого підходу – або

їх комбіноване застосування – залежить від характеру об'єкта, типу загроз, специфіки регіону, а також управлінських потреб і політик у сфері безпеки.

Основні критерії, за якими можна диференціювати вказані підходи, узагальнено в таблиці 2. Вони дозволяють структуровано оцінити, який підхід доцільніше застосовувати в тій чи іншій ситуації для досягнення максимальної ефективності в управлінні критичною інфраструктурою.

Отже, при організації системи управління критичною інфраструктурою необхідно усвідомлювати, що не існує єдиного універсального підходу, який би був ефективним у всіх умовах та для всіх типів об'єктів. Кожен елемент критичної інфраструктури є унікальним за своєю природою, має специфічні функціональні особливості, рівень взаємозалежності з іншими об'єктами, характерні загрози та вимоги до безпеки. Відповідно, підходи до забезпечення його захисту повинні адаптуватися до конкретного контексту.

Ефективне управління безпекою критичної інфраструктури потребує гнучкого поєднання різноманітних підходів – як тих, що базуються на структурно-функціональному аналізі об'єкта, так і тих, що орієнтовані на оцінку ризиків та реагування на загрози. Така комбінація дозволяє враховувати як технічні, так і організаційні аспекти захисту, створюючи умови для забезпечення високого рівня стійкості об'єктів до внутрішніх і зовнішніх викликів.

Під захистом критичної інфраструктури України слід розуміти комплекс заходів, реалізований у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури [9]. В останні роки серед основних загроз безпеці та стійкості критичної інфраструктури вагоме місце займають кібератаки.

Одночасно відбувається й поступова зміна напряму загроз: з локального та галузевого на загальнонаціональний та наднаціональний [10]. А в умовах повномасштабної війни кібератаки, які здійснювалися на критичну інфраструктуру будь-якої іншої країни у світі, за регулярністю, масовістю, глибиною та витонченістю не йдуть у жодне порівняння з кібератаками, які відбуваються на об'єкти критичної інфраструктури України [11].

Таблиця 2 – Критерії розмежування підходів до ідентифікації об'єктів критичної інфраструктури

Критерії	**Підходи до ідентифікації об'єктів критичної інфраструктури**	
	1 група	**2 група**
Основна мета оцінки об'єктів критичної інфраструктури	Визначення якості та ефективності функціонування в контексті значення для економіки та суспільства.	Визначення потенційних загроз і розробка відповідного реагування.
Методи оцінки об'єктів інфраструктури	Допомагають дослідити основні аспекти функціонування інфраструктури для визначення впливу на соціально-економічну сферу та оточуюче середовище.	Дозволяють оцінити ризики, пов'язані з інфраструктурою, та прийняти необхідні заходи для забезпечення її стійкості та безпеки.
Орієнтація на вплив на економіку та суспільство	Економічний вплив і соціальний вплив є значущими для обох груп, оскільки вони визначають важливість об'єктів для економіки та суспільства.	
Регуляторні та нормативні вимоги	Відповідність нормативам та законодавча база є важливими для обох груп, оскільки вони впливають на визначення стандартів безпеки та відповідність законодавчим вимогам.	
Стратегії управління кризовими ситуаціями	Включають розробку планів надзвичайних ситуацій, постійний моніторинг стану інфраструктури, швидке реагування на кризові ситуації, відновлення функціонування після кризи і проведення аудиту для подальшого вдосконалення стратегій управління.	Включають заходи запобігання (профілактичні заходи), заходи мінімізації наслідків (плани евакуації, резервування даних), а також підготовку до реагування під час кризових ситуацій.

Вищевказані зміни здійснюють вплив і на управлінські дії в сфері кібербезпеки. Адже тривалий час ефективно знижувати рівень кіберзагроз, як ключових загроз безпеці, означало систематично знищувати бізнес-модель, за якою в умовах невисокого ризику нескладні для застосування інструменти використовуються для отримання значних прибутків [12]. У такій ситуації головною метою ефективного кіберзахисту було створення умов, за яких здійснення кібератаки ставало економічно невигідним для зловмисника, насамперед у фінансовому вимірі. Саме тому підприємства та інші суб'єкти господарювання зосереджувалися не лише на впровадженні технологічних рішень у сфері кібербезпеки, а й на системному аналізі власних цифрових активів з позиції їх уразливості та потенційних фінансових наслідків у разі компрометації. Така оцінка охоплювала як прямі, так і непрямі ризики: можливі репутаційні втрати, витік конфіденційної інформації, персональних даних працівників і клієнтів, злам фінансових систем, паралізацію роботи серверів або недоступність веб-ресурсів.

Однак упродовж останніх років кіберпростір став однією з ключових арен гібридної війни, що спричинило ескалацію кіберзагроз на якісно новий рівень. Кібератаки дедалі частіше набувають ознак цілеспрямованого впливу, ініційованого геополітичними гравцями або підтримуваного державними структурами. У таких випадках економічні міркування, як-от фінансова вигода чи рентабельність атаки, відходять на другий план або взагалі втрачають значення.

Метою подібних атак може бути дестабілізація функціонування критичної інфраструктури держави, порушення роботи урядових або військових систем, розповсюдження дезінформації, підрив довіри до державних інститутів чи порушення безпеки міжнародних партнерів. Відтак, рівень загроз значно зростає, і заходи з кіберзахисту мають адаптуватися до нових умов – передусім, шляхом посилення міжвідомчої координації, інтеграції національних і міжнародних стратегій безпеки.

Для формування пропозицій щодо покращення системи кіберзахисту критичної інфраструктури України, необхідно спочатку ідентифікувати увесь спектр потенційних кіберзагроз, а також їхні

джерела. Закон України «Про основні засади забезпечення кібербезпеки України» визначає кіберзагрози як наявні та потенційні явища і фактори, що становлять небезпеку життєво важливим національним інтересам України у кіберпросторі та негативно впливають на стан кібербезпеки держави [13].

В юридичній практиці під кіберзагрозою також розуміють протиправні, карані дії суб'єктів інформаційних правовідносин, які створюють небезпеку життєво важливим інтересам людини, суспільства та держави в цілому, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, а також відносинам щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [14].

З точки зору необхідності генерації відповідних управлінських рішень варто зрозуміти, що кіберзагрози виникають у результаті комплексу факторів, які створюють сприятливі умови для атак на інформаційні системи та інфраструктуру. В першу чергу мова йде про швидкий розвиток інформаційних технологій, що значно розширює цифровий простір та надає зловмисникам більше можливостей для впровадження шкідливих дій. Постійне зростання кількості підключених до мережі пристроїв (Інтернет речей) також створює нові вектори для атак, оскільки багато з них мають вразливості у системах безпеки [15; 16].

Другою умовою є людський фактор, який включає помилки користувачів, недостатній рівень кіберграмотності та невідповідне управління паролями. Важливу роль відіграє і соціальна інженерія, що спрямована на маніпулювання людьми з метою отримання доступу до конфіденційної інформації [17].

Третьою умовою є недостатній рівень захисту інформаційних систем. Вказана ситуація може бути викликана як застарілими технологіями, так і відсутністю сучасних засобів захисту, таких як міжмережеві екрани, системи виявлення та запобігання вторгненням, а також антивірусні програми. Відсутність регулярних оновлень програмного забезпечення також створює додаткові ризики [18–20].

Четвертою умовою є складність та взаємозалежність сучасних інформаційних систем, що ускладнює їхній захист і робить системи

більш вразливими до комплексних атак. Взаємозалежність означає, що уразливість в одній частині системи може призвести до компрометації інших частин [21].

П'ятою умовою є економічні та політичні мотиви зловмисників. Кіберзлочинці можуть бути мотивовані фінансовою вигодою, викраденням інтелектуальної власності або дестабілізацією роботи підприємств, що належать до критичної інфраструктури з політичних міркувань. Державні актори також можуть використовувати кібератаки для проведення шпигунських операцій або кібервійни [22–24].

Розгляд та систематизація існуючих кіберзагроз [25–29] в контексті впливу на діяльність об'єктів критичної інфраструктури надає можливість сформувати набір ознак для їхньої класифікації (табл. 3).

Таблиця 3 – Класифікація кіберзагроз критичній інфраструктурі

Класифікаційна ознака	**Види**
За типом загроз	Шкідливе програмне забезпечення. Мережеві атаки, такі як DoS, DDoS, та MitM. Фішинг та інші методи соціальної інженерії. Зловмисні дії інсайдерів.
За метою атак	Крадіжка даних. Знищення або пошкодження інфраструктури. Кібершпигунство з економічних чи політичних мотивів. Пряма фінансова мотивація.
За джерелом загроз	Зовнішні загрози. Внутрішні загрози.
За об'єктом впливу	Атаки, спрямовані на фізичні компоненти інфраструктури. Атаки на інформаційні системи, дані та мережі.

Зазначені класифікаційні ознаки дозволяють системно структурувати кіберзагрози не лише для глибшого розуміння їхньої сутності, але й для пошуку найбільш дієвих засобів та інструментів протидії. Створення ефективної системи кіберзахисту неможливе без усвідомлення реальних і потенційних загроз, постійного вдосконалення засобів оборони, а також інтеграції безпекових підходів у всі

операційні та управлінські процеси підприємств, що належать до критичної інфраструктури.

З огляду на вищезазначене побудова ефективної системи кіберзахисту критичної інфраструктури має ґрунтуватися на комплексному підході, який включає технічну, організаційну та правову аспекти складові, а його реалізація потребує відповідних управлінських рішень (рис. 2).

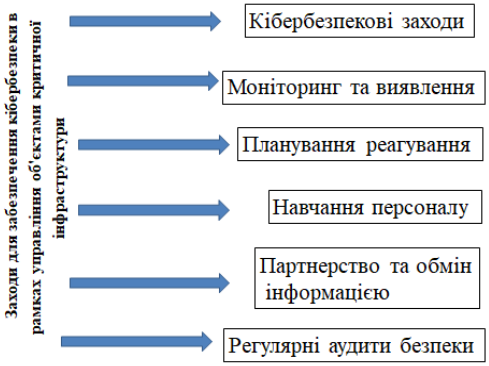

Рисунок 2 – Заходи щодо забезпечення кіберзахисту об'єктів критичної інфраструктури

Звісно, використання виключно управлінських інструментів не в змозі забезпечити захист критичної інфраструктури. Одночасно необхідно впроваджувати передові технології захисту, а також здійснювати регулярне оновлення та патчінг систем. Окремим напрямом можна виділити заходи мережевої безпеки, яка включає захист мережевого трафіку за допомогою інтрузивних систем виявлення та запобігання інтрузіям (IDS/IPS) та використання віртуальних приватних мереж (VPN) для захисту комунікацій. І, нарешті, захист даних, який включає шифрування чутливих даних під час зберігання та під час передачі, також забезпечення регулярних резервних копій та захист від втрати даних. Технічною складовою кіберзахисту об'єктів критичної інфраструктури опікується й держава, адже власник та/або керівник об'єкта критичної інфраструктури організовує невідкладне інформування урядової команди реагування на комп'ютерні

надзвичайні події України CERT-UA (у разі наявності – галузевої команди реагування на комп'ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об'єкта [30].

Серед організаційних заходів на підприємствах, що належать до критичної інфраструктури ключову роль відіграє робота з персоналом. Вона обов'язково має включати регулярне навчання співробітників, проведення тренувань і симуляцій кібератак (пентестів), а також розвиток корпоративної культури кібербезпеки. На рівні окремих працівників, особливо тих, хто має доступ до конфіденційної інформації, важливою є свідомість і готовність звітувати про потенційні кіберзагрози та кіберінциденти.

З огляду на вищевказане, в Україні трансформація управлінських систем та прийняття рішень у сфері захисту критичної інфраструктури від кіберзагроз має відбуватися в рамках наступних напрямків (рис. 3).

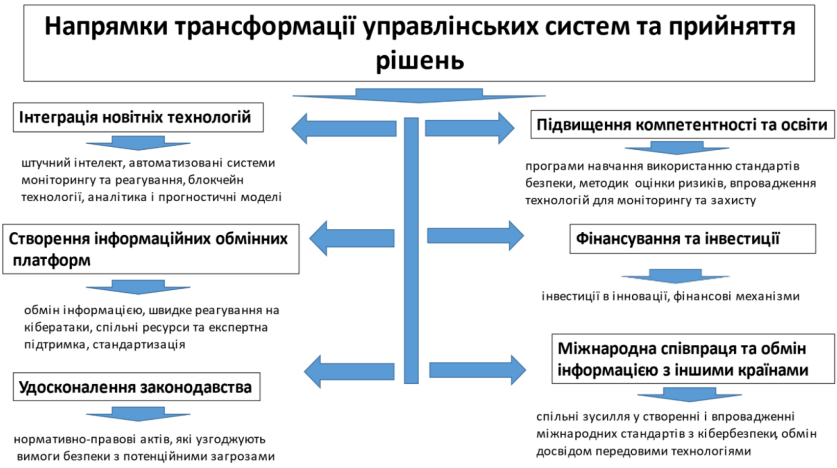

Рисунок 3 – Напрямки трансформації управлінських систем та прийняття рішень у сфері захисту критичної інфраструктури в контексті кіберзагроз

В управлінському контексті особливе значення має підготовка висококваліфікованих менеджерів, здатних не лише орієнтуватися в сучасних умовах цифрової загрози, а й ефективно застосовувати новітні інструменти управління для забезпечення безпеки критичної інфраструктури. З урахуванням зростаючої складності кіберзагроз, сучасний керівник повинен вміти приймати обґрунтовані рішення, аналізувати ризики, ініціювати впровадження технологічних рішень та координувати дії між різними суб'єктами безпеки. Для цього необхідним є запровадження спеціалізованих освітніх модулів з питань кібербезпеки у навчальні програми як технічного, так і управлінського спрямування. Такий міждисциплінарний підхід дозволить формувати керівників нового покоління, які володітимуть як глибокими фаховими знаннями, так і стратегічним баченням у сфері кіберзахисту.

Крім формальної освіти, важливим елементом підвищення управлінської спроможності є організація практико-орієнтованих заходів – тренінгів, семінарів, стратегічних сесій для керівного складу підприємств, що належать до критичної інфраструктури. Такі заходи мають бути спрямовані на опанування сучасних знань про типи кіберзагроз, способи їх виявлення, локалізації та нейтралізації, а також на розвиток навичок кризового управління в умовах кібератак. Додатковим ресурсом для підвищення наукової та практичної обґрунтованості рішень у сфері кібербезпеки має стати створення дослідницьких центрів, які б займалися розробкою інструментів управління, аналітикою ризиків і впровадженням інноваційних підходів у сфері цифрової безпеки. У контексті глобального характеру кіберзагроз важливо залучати до їхнього дослідження міжнародних експертів, які можуть передати передовий досвід, забезпечити міждержавну координацію та посилити інтеграцію в міжнародну систему кіберзахисту.

Паралельно з освітньо-науковими ініціативами, надзвичайно важливим є належне фінансування системи кібербезпеки, що в умовах обмежених ресурсів та постійного оновлення технологій вимагає чітко структурованого підходу на всіх рівнях управління. Інвестування у кібербезпеку варто розглядати не лише як витрати, а як стратегічну інвестицію у стійкість і життєздатність держави.

На рівні підприємств, що належать до критичної інфраструктури управлінські рішення мають бути спрямовані на впровадження новітніх технологій, оновлення програмного забезпечення, модернізацію систем захисту даних та мереж. Таке спрямування дозволяє значно знизити вразливість до зовнішніх атак і забезпечити безперервність функціонування в умовах кризових ситуацій.

На макрорівні, в межах ІТ-галузі, варто підтримувати дослідження та розробки, спрямовані на створення нових технологій виявлення, реагування та захисту від кіберзагроз. Розвиток науково-технічного потенціалу у цій сфері є запорукою підвищення ефективності захисних механізмів та конкурентоспроможності на міжнародному рівні. Водночас на державному рівні доцільним є створення спеціального фонду підтримки інновацій у сфері кібербезпеки. Такий фонд має стати інструментом стимулювання науково-дослідницької діяльності, комерціалізації технологій, а також підтримки стартапів, які розробляють рішення для захисту критичної інфраструктури. В залежності від специфіки кожного окремого проєкту кібербезпеки фінансування може надаватися на різних етапах – від формування ідеї та концептуального рішення до етапів тестування та впровадження технологій на практиці.

Серед фінансових інструментів, які можуть (хоча й в непрямій формі) сприяти зміцненню кіберзахисту об'єктів критичної інфраструктури, можна відзначити пільгове кредитування та надання грантової підтримки. Вказані інструменти дозволяють підприємствам здійснювати модернізацію наявної системи кіберзахисту без надмірного навантаження на бюджет, а також пришвидшують оновлення технічної бази. Крім того, ефективним підходом є використання моделі державно-приватного партнерства у сфері кібербезпеки. Об'єднання фінансових ресурсів держави та бізнес-структур не лише зменшує ризики для кожної зі сторін, а й створює сприятливе середовище для впровадження інновацій та масштабування рішень, особливо у разі реалізації складних та технологічно затратних проєктів.

Окремі підприємства, що відносяться до критичної інфраструктури можуть підвищити ефективність кіберзахисту на основі управлінської складової, а саме, за рахунок інтеграції менеджменту кібербезпеки. Під останнім слід розуміти процес планування, розробки, впровадження та

керування заходами, які спрямовані на захист комп'ютерних систем, мереж і даних від наявних та потенційних кіберзагроз.

Щоб довести доцільність застосування менеджменту кібербезпеки, насамперед, потрібно зупинитися на таких його категоріях, як результативність та ефективність. В загальному вигляді результативність менеджменту є мірою ступеня реалізації певної стратегії, а ефективність є оцінкою використання ресурсів підприємства у ході її реалізації [31]. Джерелом результативності менеджменту можуть виступати певний рівень спеціалізації менеджера, диференціація видів управлінської роботи, інформаційне забезпечення, автоматизація та алгоритмізація управлінських процесів, координація спільних і функціональних дій управлінської команди [32]. В контексті результативності менеджменту кібербезпеки, яка однаково залежить, як від управлінського фундаменту, так і від надбудови пов'язаної з небезпеками кіберсередовища, має бути визначена ступінь досягнення запланованих цілей у вигляді якісних та кількісних показників. У свою чергу, ефективність менеджменту, відображає якісну властивість результативності, а її розрахунок здійснюється відношенням результату до витрат на його отримання [33]. На прикладі менеджменту кібербезпеки це виявляється в економічній недоцільності здійснення кібервтручання внаслідок наявності належної системи кіберзахисту.

Застосування менеджменту кібербезпеки на підприємствах, що належать до критичної інфраструктури вимагає активного залучення їхнього керівництва. Насамперед, мова йде про прийняття низки управлінських рішень щодо придбання продуктів та послуг кібербезпеки, формування корпоративної культури безпеки та розробки комплексу заходів, що охоплюють організаційні та технічні аспекти кіберзахисту. Робота в цьому напрямі має здійснюватися одночасно на кількох рівнях – стратегічному, оперативному та тактичному – що дозволить забезпечити узгодженість дій, гнучкість реагування та стійкість до нових форм кіберзагроз.

По-перше, оцінка ризиків, яка дозволяє визначити, які активи критичної інфраструктури піддаються кібератакам, і яким ризикам вони піддаються. По-друге, розробка політик та процедур кібербезпеки. Вони мають визначити, як саме потрібно захищати від

кібератак кожен об'єкт критичної інфраструктури. По-третє, для реалізації політики та процедур кібербезпеки необхідно встановлення брандмауерів, антивірусного програмного забезпечення та систем виявлення вторгнень. По-четверте, персонал підприємств, що належать до критичної інфраструктури має бути обізнаний про кібербезпеку та вміти запобігати кібератакам [34].

Впровадження менеджменту кібербезпеки в межах окремих підприємств, що належать до критичної інфраструктури можна розглянути як певну послідовність етапів (табл. 4).

Таблиця 4 – Етапи впровадження менеджменту кібербезпеки

Назва етапу	Характеристика етапу
Кількісна та якісна оцінка ризиків	Оцінка ризиків за допомогою методології управління ризиками в галузі кібербезпеки OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), міжнародного стандарту з управління ризиками інформаційної безпеки ISO/IEC 27005, методики кількісної оцінки ризиків FAIR (Factor Analysis of Information Risk) тощо
Формування внутрішньої політики кібербезпеки	Розробка нормативної бази з основними вимогами до кібербезпеки на підприємстві критичної інфраструктури. Це можуть бути документи із загальними правилами користування інформаційними ресурсами, визначення ролей, посад та відповідальних за кібербезпеку, правила доступу зберігання, обробки та передачі інформації тощо.
Вибір конкретних заходів забезпечення кіберзахисту	Визначення оптимальних заходів технічного чи організаційного характеру, формування бюджетів під вказані заходи.
Розробка процедур кібербезпеки	Визначаються та прописуються процедури з алгоритмом дій на випадок кіберінцидентів.
Впровадження та підтримка системи менеджменту кібербезпеки	Реалізація розроблених заходів: проведення регулярного моніторингу, оновлення програмних продуктів та безпекових політик, тренування персоналу (наприклад, за допомогою пентенстінгу), розробка навчальних програм тощо.

До початку впровадження повноцінної системи кіберзахисту на об'єктах критичної інфраструктури необхідним кроком є проведення попередньої категоризації. Категоризація передбачає не лише формальне визначення критичності, яка, як правило, закріплюється на державному рівні, але й детальніше оцінювання додаткових параметрів, що вказують на важливість конкретного об'єкта в контексті забезпечення кібербезпеки. Серед таких параметрів можна відзначити рівень залежності населення від функціонування об'єкта, його економічний вплив на регіон чи країну, роль в інформаційному обміні, стратегічне значення для суміжних галузей та інші релевантні характеристики.

Особливу увагу в процесі категоризації потрібно приділяти аналізу взаємозв'язків між об'єктами. Деякі з них можуть не виглядати критичними ізольовано, однак мати ключове значення через опосередкований вплив на функціонування інших систем або елементів інфраструктури. Таким чином, категоризація має носити не лише формальний, а й системний характер. Важливо, щоб вона залишалася динамічною, адже перелік критичних об'єктів потребує періодичної ревізії й оновлення залежно від змін у технологічному середовищі, соціально-економічній ситуації та загрозах у кіберпросторі.

Після завершення етапу категоризації можна переходити до ідентифікації та оцінки потенційних кіберзагроз, які можуть вплинути на ці об'єкти. Як уже зазначалося раніше, класифікація кіберзагроз включає низку ознак, що дозволяють глибше розуміти джерела, методи, умови та можливі наслідки атак. На цьому етапі важливо не лише провести одноразову оцінку загроз, а й запровадити механізми постійного аналізу тенденцій у сфері кібербезпеки. Вказані механізми передбачають застосування моніторингу змін у характері атак, виявлення нових інструментів кіберзлочинців, адаптацію до змін у законодавстві та міжнародних стандартах.

У практичному вимірі таке спостереження реалізується через аналіз звітів про кіберінциденти, участь у профільних конференціях та форумах, співпрацю з галузевими експертними спільнотами та кіберрозвідувальними організаціями. Водночас має здійснюватися регулярний аудит систем кіберзахисту, який включає оцінювання ефективності наявних політик, процедур, технічних засобів захисту та їх відповідності чинним стандартам.

Результати оцінки кіберзагроз та аудиту кіберзахисту слугують підгрунтям для розробки або адаптації стратегій управління ризиками. Зазначений процес охоплює планування оновлень програмного забезпечення, модернізацію технічних рішень, розробку нових внутрішніх регламентів, а також регулярне навчання персоналу, що дозволяє підвищити готовність до реагування на кіберінциденти.

Управління ризиками критичної інфраструктури має бути безперервним, з орієнтацією на мінімізацію потенційних втрат та забезпечення сталості функціонування ключових об'єктів в умовах постійно змінюваного кіберсередовища. Комплексний підхід до категоризації, ідентифікації загроз, аудиту безпеки та управління ризиками формує основу надійної системи кіберзахисту, здатної ефективно відповідати на сучасні виклики.

Вибір продуктів/послуг, заходів та інструментів для забезпечення кібербезпеки залежить від кожної конкретної ситуації і знаходиться більше в компетенції технічних фахівців, але, в будь-якому випадку, кінцеве управлінське рішення та подальше виділення ресурсів – це все ж прерогатива менеджменту (табл. 5).

Однак навіть при забезпеченні надійного кіберзахисту в технологічному аспекті, не можна забувати й про вплив людського чиннику. Часто працівники підприємств, що належать до критичної інфраструктури мають низький рівень обізнаності щодо кібербезпеки, що підвищує ризик успішних атак. На практиці можна спостерігати недостатнє розуміння основних принципів кібербезпеки, незнання актуальних загроз та методів захисту, працівники просто можуть не знати, як правильно реагувати на потенційні кіберінциденти, що може призвести до запізнілих дій і посилення наслідків атаки.

Крім того, в штатному розкладі підприємств, які належать до критичної інфраструктури нечасто можна спостерігати окрему керівну посаду відповідального за управління кіберзахистом. Зазвичай, такі функції виконує хтось з технічних фахівців – системний адміністратор, консультант з IT-безпеки, дизайнер систем мережевої безпеки, фахівець з безпеки тощо.

Хоча, з іншого боку, згідно «Переліку базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури» кожен такий об'єкт повинен мати у своєму складі підрозділ або посадову особу з інформаційної безпеки, що відповідають за політику інформаційної безпеки,

прийняту на об'єкті критичної інфраструктури, та контроль за її дотриманням. Під час визначення відповідальних за інформаційну безпеку перевага має надаватися особам, які мають фахову освіту та досвід роботи у сфері технічного захисту інформації або інформаційної безпеки [35].

Таблиця 5 – Умови прийняття управлінських рішень щодо придбання продуктів та послуг кібербезпеки

Характеристика	Опис
Персоніфікація запитів.	Замовник бажає отримати індивідуальне рішення, наприклад, з урахуванням рівня критичності об'єкту, особливостей сфери діяльності, бізнес-процесів.
Варіативність рішень.	На ринку пропонується значна кількість універсальних та галузевих безпекових рішень на різний бюджет, а також послуги у сфері кіберзахисту пропонують окремі розробники та інтегратори.
Технічне погодження.	Хоча презентація безпекових рішень, зазвичай, проводиться перед керівництвом, підсумкове рішення щодо придбання обов'язково погоджується із технічними фахівцями.
Значні бюджети замовлень	Нормальне функціонування більшості об'єктів критичної інфраструктури напряму залежить від рівня кіберзахисту, відповідно і ціна продуктів та послуг кібербезпеки може бути значною.
Запит щодо комплексного захисту.	Причини виникнення та джерела кіберзагроз є різними, але замовник зазвичай вимагає універсальне рішення, яке гарантує максимально ефективний захист на будь-який випадок.
Бажання швидкого виконання	Керівництво здебільшого осмислює потребу у кібербезпеці лише після інциденту і підрахування втрат від нього. І вже тільки потім витрачає гроші на продукти/послуги кібербезпеки, щоб унеможливити або мінімізувати втрати у майбутньому.

Серед конкретних інструментів, що демонструють високу ефективність у практичному навчанні та підготовці персоналу до реагування на кіберінциденти, особливо виділяються симуляції. Вказані тренінги дозволяють моделювати різноманітні сценарії кібератак – від базових форм фішингу до складних ситуацій із витоком даних чи

зловмисним проникненням у мережі. Завдяки використанню спеціалізованих програмних засобів, симуляції створюють максимально реалістичні умови, які дають змогу не лише перевірити готовність персоналу, але й оцінити дієвість внутрішніх процедур безпеки. Після завершення імітації атаки проводиться детальний аналіз дій учасників та їх відповідності встановленим протоколам, що дозволяє виявити слабкі місця та вносити, за необхідністю корективи у навчальні програми і політики безпеки.

У контексті ефективного управління кіберзахистом критичної інфраструктури важливе значення має створення Центрів моніторингу безпеки – Security Operations Center (SOC). SOC забезпечує цілодобовий контроль за подіями у мережі, аналіз потенційних загроз та оперативне реагування на кіберінциденти. Такий центр функціонує як центральний вузол збору та обробки інформації про безпекові події, що дозволяє швидко локалізувати атаки і мінімізувати їхні наслідки для роботи критичних систем. Завдяки координації дій фахівців різного профілю SOC сприяє підвищенню загального рівня кіберстійкості інфраструктури.

Не менш важливим елементом системи кіберзахисту є розробка та впровадження детальних тактичних планів реагування на кіберінциденти. Вказані документи регламентують послідовність дій у разі виявлення загрози чи атаки, включаючи процедури оповіщення відповідальних осіб, ізоляції уражених систем та заходи щодо їх відновлення. Планування таких заходів дозволяє зменшити час реагування, забезпечити безперервність роботи інформаційних ресурсів та мінімізувати збитки для організації.

З огляду на особливості функціонування об’єктів критичної інфраструктури, не менш важливою складовою їхнього кіберзахисту є наявність надійного нормативно-правового та інституційного фундаменту. Важливою складовою цього процесу є адаптація міжнародних стандартів кібербезпеки, таких як ISO/IEC 27001, до національних умов і законодавства за допомогою визначення конкретних стандартів та вимог щодо захисту інформаційних систем, що мають стратегічне значення для безпеки держави та економіки.

Розробка та впровадження відповідних нормативних актів забезпечує єдність підходів до захисту інформаційних активів на національному рівні, сприяє гармонізації українських стандартів із міжнародними та підвищує

загальний рівень кібербезпеки. В результаті створюється система, здатна ефективно протидіяти сучасним викликам у кіберпросторі та гарантувати стабільність функціонування критично важливих об'єктів.

На основі сформульованих в дослідженні припущень можна сформувати концептуальну модель інтеграції принципів та інструментів менеджменту кібербезпеки в діяльність об'єктів критичної інфраструктури України (рис. 4).

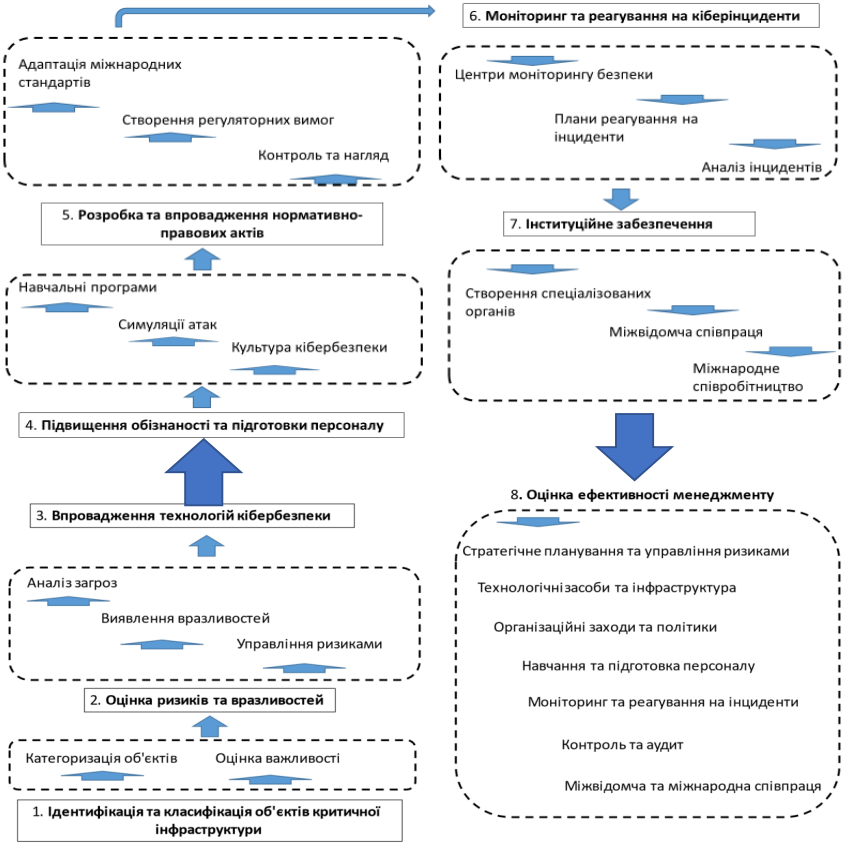

Рисунок 4 – Концептуальна модель інтеграції менеджменту кібербезпеки в діяльність об'єктів критичної інфраструктури України

Розробка та впровадження запропонованої концептуальної моделі забезпечить підвищення рівня захисту критичної інфраструктури України, зменшення ризиків кіберзагроз та в цілому сприятиме стійкості та безпеці суспільства в умовах сучасних викликів.

Висновки. Об'єкти критичної інфраструктури мають надзвичайне значення для національної безпеки, оскільки забезпечують безперебійну роботу ключових систем – енергопостачання, транспорту, зв'язку, водопостачання та водовідведення. Водночас, вказані об'єкти постійно стикаються з різноманітними ризиками, серед яких особливе місце займають загрози, пов'язані з кіберпростором. Сучасні виклики змушують розглядати питання кіберзахисту не лише з технічної точки зору, а й у контексті управлінських рішень, що включають формування адекватних бюджетів, створення ефективних організаційних структур, належну підготовку кадрів, а також впровадження механізмів планування, контролю і координації дій.

Для організації надійного кіберзахисту критичної інфраструктури необхідний комплексний підхід, який об'єднує зусилля на всіх рівнях – від урядових інституцій до окремих підприємств. Такий підхід дозволяє своєчасно запобігати кіберзагрозам і ефективно реагувати на кіберінциденти, що можуть суттєво вплинути на функціонування життєво важливих систем. Водночас комплексність означає не просто технічні заходи, а й продуману організаційну та управлінську стратегію.

У майбутньому зростання потреб у продуктах і послугах кібербезпеки буде стимулювати тіснішу співпрацю між державними органами, місцевою владою, бізнес-структурами, науковими установами, освітніми закладами, стартапами та окремими розробниками. Така взаємодія стане ключовою для обміну знаннями, впровадження передових технологій і кращих практик, що, в свою чергу, сприятиме загальному підвищенню рівня кіберзахисту критичної інфраструктури та забезпеченню стабільності функціонування важливих для держави систем у цифровому середовищі.

Список використаних джерел

1. Газдайка-Васильшин І. Б. Основні терміни проєкту Закону України «Про критичну інфраструктуру та її захист». *Право і суспільство*. 2019. Вип. 9. С. 15–20.

2. Франчук В. І., Пригунов П. Я., Мельник С. І. Безпека об'єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. *Соціально-правові студії.* 2021. Вип. 3. С. 142–148.

3. Лойко В. В., Храпкіна В. В., Маляр С. А., Руденко М. В. Економіко-правові засади забезпечення захисту критичної інфраструктури. *Фінансово-кредитна діяльність: проблеми теорії і практики.* 2020. № 4. С. 426–438.

4. Бірюков Д. С., Кондратов С. І., Насвіт О. І., Суходоля О. М. Зелена книга з питань захисту критичної інфраструктури в Україні. Київ : Національний інститут стратегічних досліджень, 2015. 35 с.

5. Єрменчук О. П. Поняття критична інфраструктура. *Інформаційна безпека людини, суспільства, держави.* 2018. № 1. С. 20–28.

6. Теленик С. С. Державна система захисту критичної інфраструктури України: концептуальні засади адміністративно-правового регулювання. Херсон : Видавничий дім «Гельветика», 2020. 602 с.

7. Ящук В. І. Принципи проєктування автоматизованих інформаційних систем управління об'єктами критичної інфраструктури. URL: http://surl.li/stkfad

8. Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету міністрів України від 09.10.2020 р. № 1109. *Верховна рада.* URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

9. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / упоряд.: Д. С. Бірюков, С. І. Кондратов ; за заг. ред. О. М. Суходолі. Київ : НІСД, 2015. 176 с.

10. Горбаченко С. А. Кібербезпека як складова економічної безпеки України. *Галицький економічний вісник*. 2020. Том 66. № 5. С. 180–186.

11. Пядишев В. Г. Кібербезпека критичних інфраструктур: закордонний досвід та українські реалії. *Теоретичні та практичні аспекти забезпечення національної безпеки*. 2022. Частина 2. С. 229–234.

12. Полторак А. С., Сухорукова А. Л., Бурковська А. І. Кібербезпека в системі трансформації управління бізнес-організацією. *Трансформація менеджменту бізнес-організацій: сучасні тренди та виклики* : колективна монографія / за заг. ред. Сагайдака М. П., Соболєвої Т. О., 2021. С. 158–176.

13. Про основні засади забезпечення кібербезпеки України: Закон України від 28.06.2024 р. № 2163-VIII. *Верховна рада*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

14. Діордіца І. В. Поняття та зміст кіберзагроз на сучасному етапі. Goal, 2017. URL: http://goal-int.org/ponyattya-ta-zmist-kiberzagroz-na-suchasnomu-etapi/

15. Мінін Д. С. Підходи до визначення поняття «кібербезпека» URL: https://salo.li/87Ac1A4

16. Кіберзагрози і кібербезпека: чи здатні фахівці протистояти хакерам? 2016 URL: http://ukr.obozrevatel.com/news/34918-kiberzagrozi-i-kiberbezpeka-chi-zdatnifahivtsi-protistoyati-hakeram.htm

17. Лісовська Ю. Кібербезпека: ризики та заходи : навч. посіб. Київ : Кондор, 2019. 272 с.

18. Свердлик З. Кібербезпека та кіберзахист: питання порядку денного в українському суспільстві. *Український журнал з бібліотекознавства та інформаційних наук.* 2022. № 10. С.175–188.

19. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Товари і ринки*. 2022. № 3. С. 47–59.

20. Вишнівський В. В., Пампуха А. І. Кібербезпека в Україні. *Цифрова трансформація кібербезпеки*: науково-практична інтернет-конференція, 20 квітня 2022, Державний університет телекомунікацій Навчальнонаукового інституту захисту інформації. Київ, 2022. С. 31–33.

21. Кузьменко О., Маклюк О., Чернишова О. Кібербезпека бізнесу під час війни. *Економіка та суспільство*. 2022. № 44. С. 15–19.

22. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань ; упоряд. О. Довгань, Л. Литвинова, С. Дорогих ; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України» ; Національна бібліотека України ім. В. І. Вернадського. Київ, 2023. № 7 (липень). 270 с.

23. Кіберризики: як розуміти та управляти. *10 Guards*. URL: https://10guards.com/ua/articles/cyber-risks/

24. Веселова Л. Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни : дис. … доктора юридичних наук : 12.00.07 адміністративне право і процес; фінансове право; інформаційне право. Одеський державний університет внутрішніх справ. Одеса, 2021. С. 18.

25. Діордіца І. В. Класифікація кіберзагроз та їх легітимація у нормативно-правових актах України. *Підприємництво, господарство і право*, 2017. № 10. С. 206–211.

26. Діордіца І. В. Поняття і зміст кіберзагроз на сучасному етапі. *Підприємництво, господарство і право*, 2017. № 4. С. 99–107.

27. Нова стратегія кібербезпеки: як Україна захищатиметься в кіберпросторі? *Аналітичний центр ADASTRA*. URL: https://adastra.org.ua/blog/nova-strategiya-kiberbezpeki-yak-ukrayina-zahishatimetsya-v-kiberprostori.

28. Про затвердження Положення про організаційно-технічну модель кіберзахисту : Постанова Кабінету Міністрів України від 29.12.2021 № 1426. *Верховна рада України.* URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text

29. Даник Ю. Г., Дупелич С. О. Стратегічні аспекти боротьби з робототехнічними комплексами. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2017. № 2 (29). С. 16–25.

30. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету міністрів України від 19.06.2019 р. № 518. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

31. Міська Г. Сутність поняття результативність та ефективність в менеджменті. *Науковий вісник Одеського національного економічного університет* : збірник наукових праць, 2020. № 3–4. С. 97–102. DOI: 10.32680/2409-9260-2020-3-4-276-277-97-102

32. Кузнєцов Е. А. Управлінський капітал: майстер-клас: матер. магіст. семінару. Одеса : Фенікс, 2020. 118 с.

33. Сахацький М. П., Казанджі А. В. Теоретико-методичні засади оцінки результативності управління виробничо-господарською діяльністю підприємства. *Фінансово-кредитна діяльність: проблеми теорії та практики.* 2017. № 1. С. 135–141.

34. Павук І. В., Кобилкін Д. С. Особливості формування концепції управління проєктними ризиками на об'єктах критичної інфраструктури. *Інновінг сучасних трендів в менеджменті безпеки*: матеріали всеукраїнської науково-практичної конференції. м. Львів. 26 травня 2023 року. Львів, 2023. С. 59–60.

35. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету міністрів України від 19.06.2019 р. № 518. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text