УДК 342.951

ФЕДІЄНКО О.П., здобувач наукового ступеня.
ORCID: https://orcid.org/0009-0008-5383-3504.

ЕВРОПЕЙСЬКИЙ ДОСВІД ЗАКОНОДАВЧОГО ЗАБЕЗПЕЧЕННЯ ПОСИЛЕННЯ КІБЕРСТІЙКОСТІ

Анотація. *Розглянуто поняття та зміст кіберстійкості. Визначено особливості, які характеризують кіберстійкість. Деталізовано співвідношення між поняттями "кібербезпека" та "кіберстійкість". Визначено інфраструктуру кіберстійкості та її складові. Проаналізовано сучасне законодавство ЄС, присвячене питанням посилення кіберстійкості. Визначено позитивні аспекти посилення кіберстійкості у законодавстві ЄС. Особлива увага приділяється розгляду Директиви NIS2 та Закону ЄС "Про кіберстійкість". Визначено складові компоненти комплексної стратегії кіберстійкості на локальному рівні. Охарактеризовано шляхи Європейського центрального банку (ЄЦБ), спрямовані на посилення кіберстійкості банківської системи ЄС. На підставі узагальнення позитивного європейського досвіду окреслено перспективи удосконалення та посилення кіберстійкості в Україні.*

Ключові слова: *кіберстійкість, кіберпростір, кіберінцидент, кіберзахист, кібербезпека, кіберризики, ландшафт кіберзагроз, вразливість, хакер, програмне забезпечення.*

Summary. *The concept and content of cyber resilience are considered. characterizing features of cyber resilience are defined. The relationship between the concepts of cyber security and cyber resilience is detailed. Cyber resilience infrastructure and its components are defined. The current EU legislation on strengthening cyber resilience is analyzed. The positive aspects of strengthening cyber resilience in EU legislation have been identified. Special attention is paid to the review of the NIS2 Directive and the EU Cyber Resilience Act. The constituent components of a comprehensive cyber resilience strategy at the local level have been determined. The directions of the European Central Bank (ECB) aimed at strengthening the cyber resilience of the EU banking system are described. Based on the generalization of positive European experience, prospects for improving and strengthening cyber resilience in Ukraine are outlined.*

Keywords: *cyber resilience, cyberspace, cyber incident, cyber defense, cyber security, cyber risks, cyber threat landscape, vulnerability, hacker, software.*

Постановка проблеми. Перший в історії світовий рейтинг кіберзлочинності, створений у рамках дослідження Оксфордського університету, який був опублікований на початку 2024 року, підтвердив лідерський статус росії як держави-злочинця. Відповідно до оцінки світового рейтингу кіберзлочинності (World Cybercrime Index) російські кіберзлочинці вважаються найпрофесійнішими та технічно найбільш кваліфікованими у світі, і їхні злочини мають найбільший вплив [1]. В умовах масштабної кібервійни функціонування більшості сучасних автоматизованих інформаційних систем, особливо таких, що експлуатують мережеві технології перебуває у фокусі різноманітних за інтенсивністю деструктивних впливів. Підготовлені кіберзлочинці впливають через мережі та пристрої на інформаційні технології, що вимагає постійного удосконалення кібербезпеки.

На цьому фоні переважна більшість країн світу, у тому числі й держави ЄС опікуються питаннями створення та ефективного функціонування механізмів забезпечення кібербезпеки, яка має такі інституційні ознаки: формуються відповідні

правові норми переважно у форматі доктрин (стратегій) кібербезпеки та відповідних спеціальних актів законодавства, розробляються пріоритетні засади державної політики у сфері забезпечення кібербезпеки, створюються уповноважені державні структури (органи), які відповідають за стан забезпечення кібербезпеки, постійно вдосконалюються новітні технології захисту інформації та апаратно-програмного забезпечення в інформаційно-комунікаційних мережах тощо [2, с. 106]. У зазначеному контексті важливу роль нарівні із кібербезпекою посідає саме кіберстійкість.

Кіберстійкість – це здатність готуватися до кібератак або інцидентів, оперативно реагувати на них і швидко відновлюватися, зберігаючи при цьому конфіденційність, цілісність і доступність систем і даних. Тобто охоплюється комплексний підхід, який поєднує проактивні заходи, плани реагування на інциденти та постійний моніторинг кібер-середовища з метою пом'якшення ризиків і мінімізації впливу кіберзагроз. Кіберстійкість – це важливий підхід до захисту цифрових активів в епоху, коли актуалізуються та масштабуються кіберзагрози. Парадигма захисту від нових загроз є критично важливим компонентом кіберстійкості, що вимагає адаптації, передбачаючи не лише поточні загрози, але й готовність до майбутніх потужних викликів. Наприклад, зростання кількості складних кібератак, керованих штучним інтелектом (далі – ШІ), вимагає перспективного та виваженого підходу, коли механізми захисту мають постійно оновлюватися та удосконалюватися. Завдяки інтеграції передових технологій, безперервному навчанню та стратегічному плануванню розвивається кіберстійкість, яка не лише протидіє сьогоднішнім загрозам, але й має адаптуватися до невідомих викликів завтрашнього дня. Цей проактивний підхід до змісту кібербезпеки гарантує, що організації не просто реагують на загрози, але завжди грають на упередження, тобто знаходяться на крок попереду, готові протидіяти та пом'якшувати ризики в умовах динамічної цифрової ери.

Інфраструктура кіберстійкості включає елементи кібербезпеки, управління ризиками, забезпечення безперервності та реагування на інциденти. У світових вимірах, на відміну від кібербезпеки, кіберстійкість виходить за рамки технічних міркувань і зосереджена на розробці ефективної імунної системи для кожної цифрової сфери, будь то державний або приватний сектор. Ризик оцінюється та зменшується, щоб обмежити вплив інциденту, швидко виявити загрози, забезпечити продовження роботи критичних програм, зберегти дані та швидко відновити роботу у штатному режимі. Кіберстійкість характеризується безперервністю та перманентністю роботи, гарантується постійною ідентифікацією, захистом, виявленням, реагуванням на інциденти і відновленням систем. Кіберстійкість означає готовність до неминучого порушення стану кібербезпеки та усвідомлення того факту, що кожна система має реальні та потенційні уразливості.

Загальноприйнятими елементами кіберстійкості є: управління, права доступу, сегментування, забезпечення цілісності та конфіденційності даних, активне реагування на кіберінциденти, відновлення, скоординований захист. Такий підхід ґрунтується на кращих практиках побудови і управління кібербезпекою, зокрема, на методологіях, затверджених Національним інститутом стандартів і технологій США (NIST). Кожна категорія представляє собою комплекс процесів, інструментів і контролів, які формують основу управління як кіберстійкістю, так і кібербезпекою. Категорія відновлення кіберстійкості базується на стандартних процесах відновлення після збоїв (DRP) і планування безперервності ведення бізнесу (BCP). Склад контролів і заходів, впроваджуваних в цій категорії забезпечує резервне копіювання і відновлення даних, інформаційних систем та активів, а також оперативне і аварійне відновлення процесів

після кіберінциденту або кібератаки. Важливим фактором кіберстійкості є постійний перегляд і розвиток процесів відновлення систем відповідно до нових кіберзагроз.

Одночасно кіберстійкість являє собою здатність захищати та уникати катастрофічних наслідків кібератак, які проводяться за допомогою програм-вимагачів, шпигунського та шкідливого програмного забезпечення чи інших загроз від зовнішніх зловмисників. З іншого боку, кіберстійкість означає здатність суттєво зменшувати масштаби збитків та швидко запускати критично важливі операційні системи після їхнього зламу. Кіберстійкість може стосуватися як зовнішніх загроз, таких як хакери, програми-вимагачі, так і внутрішніх загроз, таких як ризик випадкового видалення або знищення службової або конфіденційної інформації тощо.

Таким чином, актуальним видається проведення дослідження з метою висвітлення кращих практик європейського досвіду у сфері забезпечення кіберстійкості, у зв'язку з чим розгляд сучасної європейської моделі законодавчого забезпечення кіберстійкості є своєчасним, заслуговує на увагу, особливо в умовах кібервійни, яку третій рік поспіль веде держава-агресор проти України.

Результати аналізу наукових публікацій. На науково-методичному рівні проблематику забезпечення кіберстійкості розглядали: М. Костроміна та Л. Гарнатко [3], О. Користін і С. Демедюк [4] та інші. Кіберстійкість об'єктів критичної інфраструктури перебувала у фокусі уваги таких науковців: М. Комарова [5], І. Мальцевої [6], В. Шиповського [7]. Деякі питання організаційно-правового забезпечення кіберстійкості на європейському рівні вивчали такі представники європейської правової школи, як А. Симона [8], К. Лауренс [9]. Проте висвітлення законодавчих ініціатив на рівні ЄС у сфері розбудови кіберстійкості ретельно вказаними авторами не досліджувалося, що засвідчує актуальність тематики цієї наукової статті.

Метою статті є висвітлення особливостей забезпечення посилення кіберстійкості на європейському рівні на підставі аналізу сучасних актів законодавства ЄС та перспектив удосконалення європейської моделі посилення кіберстійкості.

Виклад основного матеріалу. Ефективне управління кіберстійкістю є досить складним процесом, який вимагає розуміння та вирішення широкого спектру взаємопов'язаних систем, процесів і технологій. Ця складність може бути надзвичайною для структур з обмеженими ресурсами або невеликим досвідом у сфері кібербезпеки. Іншим значним викликом є ландшафт кіберзагроз, що швидко змінюється. У поєднанні з обмеженнями ресурсів, таких як бюджет, досвід і технології, організаціям може бути важко залишатися в курсі проблем і відповідним чином адаптувати свої засоби захисту. Окрім вказаного, додаткові виклики включають: швидкий технологічний розвиток; відсутність процесів стандартизації; складність нових технологій, таких як IoT або Хмарні обчислення; інсайдерські загрози та недбалість співробітників; геополітичні зміни; обмежені дані про кіберзагрози; організаційна відокремленість і відсутність співпраці.

У сучасному ландшафті кіберзагроз, який постійно змінюється, кіберстійкість є надзвичайно важливою. Кіберстійкість допомагає проактивно захищатися від кібератак і мінімізувати вплив потенційних зломів. Шляхами посилення загальної кіберстійкості є:

1) Створення передумов задля візуалізації пристроїв в режимі реального часу, оскільки ця функція забезпечує пасивне профілювання для чутливих систем, безперервний моніторинг з метою обізнаності про ситуацію та інвентаризацію в реальному часі всіх пристроїв без порушення критичних процесів;

2) Автоматизоване застосування політики нульової довіри "ZeroTrust" з метою організації доступу з найменшими привілеями для всіх керованих і некерованих

пристроїв, включаючи IT, OT, IoT, IioT та IoMT-пристрої. Застосування елементів керування на основі політики нульової довіри з метою забезпечення відповідності пристрою вимогам, завчасно зменшить кількість атак і надасть змогу швидко реагувати на кіберінциденти. Це також передбачає автоматизацію оцінки відповідності та запуску робочих процесів виправлення, щоб забезпечити відповідність внутрішнім політикам безпеки, зовнішнім стандартам і галузевим нормам;

3) Сегментація мережі, що надасть змогу спростити динамічну сегментацію для всіх кіберактивів, щоб мінімізувати поверхню атак і регуляторний ризик.

На цьому фоні важливим є посилення захисту пристроїв операційної технології і протоколів моніторингу, якими часто користуються хакери та зловмисники, запобігання розкриттю інформації про походження та типи атак, зокрема про протоколи OT під час скоєння нападу; вивчення наслідків після експлуатації, поширених штамів зловмисного програмного забезпечення, командно-контрольних серверів і глобального розподілу загроз, що сприятиме розрізненню опортуністичних і цілеспрямованих кібератак, підкреслення важливості постійної ідентифікації вразливостей і сегментації мережі.

У зарубіжній науковій літературі переважно кіберстійкість визначають як здатність постійно досягати запланованого результату, незважаючи на несприятливі кіберризики та кіберподії [10]. Вивчення кіберстійкості є надзвичайно важливим для організацій у всіх секторах, як державних, так і приватних, оскільки кіберстійкість необхідна для забезпечення системних процесів безперервності під час неочікуваних обставин та є джерелом виживання в кризових сценаріях. За такою логікою кіберстійкість є міждисциплінарною сферою, яка тісно пов'язана із кібербезпекою та кібератаками. Сучасна сфера та складність цифрових середовищ робить організації більш вразливими до кіберзагроз, де питання кіберстійкості постає дедалі більш важливими. Саме кібератаки вважаються однією із найсерйозніших загроз, тому завдання кіберстійкості полягають не тільки в уникненні наслідків кібератак, але й у здатності реагувати та мінімізувати їх негативний вплив, при цьому завдання збереження даних у безпеці зростає з тією ж швидкістю, що й кількість і різноманітність даних, які зберігаються в геометричній прогресії протягом багатьох років, вимагаючи від фахівців постійного пошуку альтернатив для проактивного тестування та оцінки фізичних і технічних вразливостей систем. Однак кібервразливості та кіберінциденти не тільки впливають на діяльність організацій, але й становлять зростаючу загрозу для економічної, демократичної та соціальної стійкості.

За таких умов розвиток кіберстійкості потребує переходу від звичайних заходів безпеки до еволюційних і прогностичних підходів. У той час як звичайний підхід базується на статичних заходах безпеки, еволюційний підхід надає змогу постійно покращувати кіберстійкість на основі тактики адаптивного захисту, дозволяючи організаціям на основі історії попередніх кіберінцидентів краще розуміти свої ризики та вдосконалюватись у запобіганні кібератакам. Прогнозний підхід, з іншого боку, дозволить організації використовувати дані та аналіз для прогнозування потенційних загроз, дозволяючи організації адаптуватися до нових сценаріїв і забезпечувати більш ефективні відповіді [11].

Таким чином, узагальнюючи існуючі доктринальні позиції, європейські науковці характеризують кіберстійкість чотирма основними етапами у відповідь на кризу: моніторинг – виявлення, опір – поглинання, реакція – адаптація та відновлення – реконструкція. Крім того, існує також етап підготовки – планування (до кризи) та етап навчання – оптимізації (після настання кризи). Хоча в науковій літературі немає консенсусу щодо формування етапів планування кіберстійкості та посткризового

навчання, загалом, етап підготовки – планування більше стосується управління кібербезпекою, тобто зусиль, необхідних для структурування та покращення заходів безпеки, тоді як етап навчання – оптимізація більше стосується покращення кіберстійкості системи.

Європейська спільнота дедалі більше усвідомлює масштаби та загрози для кібербезпеки, які у своїй більшості є транскордонними та переважно мають "російський слід", з яким зіткнулася й Україна. Виявлені факти багаточисельних кампаній кібершпигунства та кібератак надають підстави констатувати, що кіберпростір дедалі більше перетворюється на сферу бойових дій, де кібервійна відбувається за допомогою ботів, шкідливих програм, ботнетів та інших можливостей. Такі сучасні реалії висувають нові виклики та вимоги, які можна вважати відповідальною поведінкою будь-якої держави в кіберпросторі.

У 2018 році Європейський Парламент ухвалив резолюцію "Боротьба з кіберзлочинами", в якій зазначається, що росія і Китай через державні та недержавні інституції займаються плануванням та реалізацією кібератак на критичну інфраструктуру держав-членів ЄС [12]. У грудні 2020 року Європейська Комісія представила нову стратегію кібербезпеки ЄС [13], яка спрямована на захист глобального та відкритого Інтернету, водночас пропонуючи гарантії не лише для забезпечення безпеки, але й для захисту європейських цінностей та основних прав кожного. Стратегія містить рамкові передумови для подальших дій ЄС з метою захисту громадян та бізнесу Євросоюзу від кібернетичних загроз, сприяння розвитку захищеної інформаційної системи та щодо захисту глобального, відкритого, вільного та безпечного кіберпростору. Саме кібербезпека визначена ключовим фактором для розбудови стійкої цифрової Європи, а також для досягнення цілей стратегічної автономії ЄС за умови збереження відкритої цифрової економіки європейської спільноти. Стратегія кібербезпеки ЄС (EUCSS) має на меті гарантувати кібербезпеку на достатньому рівні та попередити можливі ризики. Ключовими пріоритетами Стратегії кібербезпеки ЄС визначено:

1) стійкість, технологічний суверенітет і лідерство;

2) розбудова оперативного потенціалу для запобігання, стримування та реагування на кіберінциденти;

3) динамічний розвиток глобального та відкритого кіберпростору шляхом посилення комплексної співпраці.

На стратегічному рівні проголошено, що держави ЄС повинні мати спроможні урядові органи, які мають контролювати кібербезпеку та які співпрацюють зі своїми колегами в інших державах-членах, обмінюючись оперативною інформацією, що є особливо важливим для секторів, які визначені як особливо критично важливі. Окреме місце у стратегії відводиться швидкому завершенню формування в ЄС комунікаційної мережі 5G, її надійному захисту та зусиллям із розвитку наступних систем зв'язку нового покоління. На стратегічному рівні планується також підвищення стандартів безпеки в мережі Інтернет, який залишається важливим інструментом задля досягнення цілей безпеки глобальних комунікацій, що передбачає використання ЄС конкурентних переваг власної промисловості, підвищення стандартів безпеки у мережах, що включає застосування сучасних систем захисту та шифрування інформації. Такий захист надаватиметься, в першу чергу, мережам правоохоронних органів та судової влади для забезпечення ефективного обміну оперативною інформацією. Ще один напрямок – створення робочих груп з кібернетичної розвідки, яка опікуватиметься прогнозуванням загроз та їх аналізом.

Майже усі європейські технологічні гіганти використовують удосконалену версію стандартів ISO/IEC 27001 та ISO/IEC 27002 з метою адекватного реагування на кіберінциденти, вирішення глобальних викликів ІТ-безпеки та підвищення цифрової довіри. Це вимагає від організацій захищати усі види інформації, розробляти централізовано керовану структуру, зменшувати витрати на неефективні захисні технології та боронити цілісність, конфіденційність і доступність своїх даних. Європейські організації, які використовують кіберстійкість, швидко стають лідерами у своїй галузі та встановлюють стандарт для своєї екосистеми, при цьому цілісний підхід стандарту ISO/IEC 27001 та ISO/IEC 27002 означає, що охоплюється вся організація, а не лише ІТ-сфера.

Практичне впровадження кіберстійкості передбачає з метою посилення захисту від кібератак, цифрових загроз і вразливостей, вимогу щодо необхідності прийняти та реалізувати кіберстійке мислення. Кіберстійкість має бути невід'ємною частиною не лише технічних систем, але й команд, організаційної культури та щоденних операцій. Тому кіберстійкість – це здатність діяти в умовах кібератаки чи іншого кіберінциденту. Це передбачуваність запровадження необхідних технічних та організаційних заходів для виявлення, реагування на такі кіберінциденти та відновлення після них, а також здатність адаптуватися та вчитися на них для покращення майбутньої стійкості.

Основним актом загальноєвропейського законодавства у сфері забезпечення кібербезпеки є Директива NIS2 (Directive on measures for a high common level of cybersecurity across the Union) [14], яка передбачає організаційно-правові заходи з метою підвищення загального рівня гарантування кібербезпеки в ЄС. Цей акт законодавства спрямований на підтримку високого рівня кібербезпеки в країнах ЄС та передбачає подальше підвищення кіберстійкості та потенціалу реагування на інциденти як державного, так і приватного секторів, і ЄС загалом. Нова директива ЄС під назвою "NIS2" замінила Директиву з безпеки мереж та інформаційних систем (Директиву NIS) та має значно посилити кібербезпеку на теренах ЄС, набувши чинності з 27 червня 2024 року.

Загальні правила кібербезпеки в ЄС, які запроваджені ще у 2016 році, були оновлені Директивою NIS2, положення якої значно модернізували існуючу законодавчу базу, сприяли контрольованості ландшафту загроз кібербезпеці. Директива NIS2 встановлює базовий рівень для заходів контролю над ризиками кібербезпеки в усіх секторах, як-от енергетика, транспорт, охорона здоров'я та цифрова інфраструктура, критична інфраструктура. Переглянута директива спрямована на гармонізацію вимог кібербезпеки та реалізацію заходів кібербезпеки в різних державах-членах ЄС. При цьому нормативно встановлюються механізми ефективної співпраці між відповідними органами в кожній державі ЄС. Тоді як у попередній Директиві NIS держави-члени були відповідальні за визначення того, які організації мають кваліфікуватися як оператори основних цифрових послуг, Директива NIS2 запроваджує загальне правило для ідентифікації організацій, що підпадають під відповідне регулювання. Водночас у тексті уточнюється, що Директива не застосовуватиметься до організацій, які провадять діяльність у таких сферах, як оборона чи національна безпека, громадська безпека та правоохоронні органи. Директива NIS2 буде застосовуватися до державних адміністрацій на центральному та регіональному рівнях, а держави-члени можуть самостійно вирішувати, що це застосовано і до адміністрацій на місцевому рівні. Окрім того, нову Директиву було приведено у відповідність із галузевим законодавством, зокрема з положенням про цифрову операційну стійкість для фінансового сектору та

директивою про стійкість критично важливих об'єктів, щоб забезпечити юридичну ясність та узгодженість між NIS2 та цими актами.

Європейський Союз на постійній основі опікується питаннями посилення кіберстійкості, з метою захисту критичної інфраструктури, комунікацій, державних інформаційних ресурсів, гарантуючи безпеку онлайн-суспільства та економіки. З цією метою було ухвалено Закон ЄС про кіберстійкість (The Cyber Resilience Act (CRA)) від 15 вересня 2022 року [15], який передбачає законодавче забезпечення покращення стану кібербезпеки за допомогою удосконалення відповідних стандартів, що передбачає створення на теренах ЄС нової європейської кібер-екосистеми, яка буде більш безпечною для усіх громадян незалежно від того, наскільки вони освідчені у питаннях цифрової безпеки. Нові правила кібербезпеки ЄС мають забезпечити посилення вимог до більш безпечного обладнання та програмного забезпечення.

Відповідно до норм цього Закону, неадекватні функції забезпечення безпеки відійдуть у минуле із запровадженням обов'язкових вимог щодо кібербезпеки для виробників і роздрібних продавців таких продуктів, причому цей захист поширюватиметься протягом усього життєвого циклу продукту. Закон гарантує гармонізовані правила виведення на ринок сучасних цифрових продуктів або програмного забезпечення; визначає рамки вимог до кібербезпеки, що регулюють планування, проектування, розробку та підтримку таких продуктів, із зобов'язаннями, які повинні виконуватися на кожному етапі; зобов'язання забезпечувати контроль протягом усього життєвого циклу таких продуктів. Закон також встановлює механізми перевірки інцидентів кібербезпеки з метою подальшої оцінки та перегляду конкретних інцидентів, імперативну вимогу щодо підготовки усіма відповідальними суб'єктами звітів про кіберінциденти та шляхи оновлення стану безпеки.

Таким чином, перш за все, на відміну від американської концепції забезпечення кібербезпеки, Закон ЄС про кіберстійкість розроблено для того, щоб змусити всіх виконувати вимоги, незалежно від того, чи це мала або велика компанія із розробки програмного забезпечення, а не лише "сертифікований виробник програмного забезпечення". Тобто на європейському цифровому ринку запроваджуються нові стандарти до вимог безпеки та особливо щодо усіх, без винятку, виробників програмного забезпечення. Згідно із законодавчими ініціативами, кібербезпека має стати важливою складовою кожного етапу процесу розробки програмного забезпечення – від планування до обслуговування. Таким чином,кожна ІТ-компанія буде змушена відстежувати та пом'якшувати будь-які вразливості протягом усього життєвого циклу цифрового або програмного продукту.

На виконання нормативних вимог, компанії будуть зобов'язані оприлюднити всю відповідну інформацію про безпеку, що включає чіткі інструкції щодо коректного встановлення та використання певного пристрою чи частини програмного забезпечення. Для компаній, які не будуть виконувати встановлені вимоги, передбачатиметься накладання штрафів у розмірі до 15 млн. Євро або 2,5 % від обігу (залежно від того, що більше). Таким чином, ЄС намагається змусити розробників створювати відповідне програмне забезпечення, яке є стійким до невизначених вірогідних кібератак. Іншим важливим наслідком цього Закону є те, що клієнтам більше не буде дозволено бути бета-тестерами цифрових продуктів або послуг, оскільки компанії будуть зобов'язані випускати лише ті продукти, які вже вільні від уразливостей та є надійними.

Деякі критики цього Закону вважають, що частини програмного забезпечення, які використовуються у комерційному програмному забезпеченні, або апаратні продукти надходять з безкоштовних загальнодоступних репозиторіїв, що відразу відносить їх до ризикованого програмного забезпечення. Покладання відповідальності на кожного

розробника програмного забезпечення вірогідно підвищить ризики. Тільки організації, які реалізують програмне забезпечення або його комбінації та можуть взяти на себе відповідальність за вироблений продукт, можуть продовжувати працювати відкрито. Програмне удосконалення для користувачів та спільні переваги безпеки глобального співробітництва в галузі програмного забезпечення будуть доступні лише розробникам, які працюють від імені кількох великих компаній. Багато сучасних розробників покладаються на програмне забезпечення з відкритим вихідним кодом із загальнодоступних репозиторіїв, не повідомляючи про це автора і тим більше не вступаючи з ним у будь-які комерційні чи договірні відносини. Якщо запропонований Закон буде застосовуватися в тому вигляді, в якому він написаний в даний час, автори можуть нести юридичну та фінансову відповідальність за те, як його компоненти застосовуються у комерційному продукті третьої сторони.

Таким чином, у європейському цифровому просторі кіберстійкість означає здатність захищати електронні дані та системи від кібератак, а також швидко відновлюватися за їхніми наслідками. Кіберстійкість – парадигма більш критична, аніж традиційна кібербезпека. Організації із ефективними можливостями у сфері кіберстійкості повинні швидко відновлювати функціонування після кібератак, технічних збоїв або спроб навмисного втручання. Кіберстійкість має на меті організацію протистояння кібератакам, технічним збоям, навмисним втручанням та швидко відновлюватися після них. Кіберстійкість забезпечується із урахуванням присутності факторів ризику, що впливають на неї та визначення переліку заходів, необхідних для впровадження з метою нівелювання наслідків проведених кібератак або іншого посягання на мережі.

Ризик кібератак ще більше посилюється високою залежністю критичної інфраструктури, фінансової системи від цифрових технологій, труднощами захисту від загроз, що швидко та динамічно змінюються, а також через те, що вони безмежні. Тому важливо, щоб уповноважені структури (банки, фінансові установи, об’єкти критичної інфраструктури) мали достатній рівень кіберстійкості задля забезпечення свого власного захисту, а також захисту всієї екосистеми. Хакери та кіберзлочинці шукають навіть крихітну вразливість у програмному забезпеченні, за допомогою якої вони можуть зламати навіть потужний кіберзахист. Зловмисники використовують уразливості в застарілому та невиправленому програмному забезпеченні для розгортання програм-вимагачів і шкідливих програм. Найбільшу стурбованість викликають саме атаки з використанням ШІ. Саме тому кіберстійкість охоплює широкий набір проактивних стратегій, практик і технологій кібербезпеки, спрямованих на локалізацію або мінімізацію впливу несприятливих кіберподій і забезпечення безперервності функціональності, навіть в умовах масштабних програмних збоїв.

За європейським законодавством кіберстійкість визначається як здатність системи захищатися від інцидентів кібератак та підтримувати належний рівень продуктивності за рахунок розвитку критичної функціональності та своєчасного відновлення якості послуг до рівня, що існував до кіберінциденту. Кіберстійкість має інтегральний характер та визначається за такими показниками як кіберживучість та кібернадійність систем. Кіберзагрози є зловмисними діями або атаками, які використовують слабкі місця в комп’ютерних системах, мережах чи цифровій інфраструктурі. Вони можуть переслідувати широкий спектр цілей, включаючи несанкціонований доступ до конфіденційної інформації, збій у роботі послуг і бізнес-операцій, фінансову вигоду або саботаж.

Щоб ефективно протидіяти цим загрозам, європейським організаціям необхідно розробити комплексну стратегію кіберстійкості на локальному рівні, яка має охоплювати такі компоненти, як:

- оцінка та управління ризиками, які допомагають визначити вразливі місця та загрози та їхній потенційний вплив на організацію та її бізнес-процеси;

- надійні засоби кібербезпеки, такі як брандмауери, системи раннього виявлення втручань, антивірусне програмне забезпечення, безпечні мережеві конфігурації, шифрування та регулярні оновлення безпеки, які захищають системи та покращують кіберстійкість;

- планування реагування на інциденти, включаючи чіткі вказівки щодо того, як реагувати, з ким зв'язуватися та які кроки необхідно вжити під час і після інциденту для захисту бізнес-операцій;

- плани забезпечення безперервності бізнесу та аварійного відновлення, включаючи підтримку резервних копій даних, створення резервних систем і регулярне тестування процедур відновлення; навчання та обізнаність співробітників, які мають зменшити ймовірність людської помилки, що призведе до успішної кібератаки;

- співпраця та обмін інформацією, що дозволяє обмінюватися найкращими практиками аналізу загроз та отриманими уроками, що сприяє підвищенню кіберстійкості;

- безперервний моніторинг і оцінка, які дозволяють організаціям виявляти й реагувати на потенційні загрози в режимі реального часу, а також визначати уразливі місця, щоб забезпечити ефективність стратегії кіберстійкості та рішень безпеки;

- регулярні оновлення та керування виправленнями, критично важливі для пом'якшення вразливостей, якими можуть скористатися кіберзлочинці;

- управління ризиками з боку третіх сторін, що дозволяє оцінювати та керувати ризиками кібербезпеки, пов'язаними зі сторонніми постачальниками або партнерами;

- управління, що означає підтримання та просування субкультури кібербезпеки та кіберстійкості в усіх структурах (організаціях) [16].

Станом на початок 2024 року лише приблизно 4 з 10 європейських компаній констатують, що вони недостатньо стійкі, щоб впоратися із складною кібератакою, і оскільки методи атак розвиваються та дедалі частіше використовують ШІ, фактична цифра, ймовірно, буде набагато вищою. Деякі компанії можуть вважати, що вони добре підготовлені, якщо мають безпечний периметр, але кіберстійкість залежить не стільки від першої лінії захисту, скільки від того, наскільки добре підприємства можуть поглинати ризики та справлятися із зростаючими кіберзагрозами, оскільки відбиття однієї кібератаки не означає наявність кіберстійкості в класичному розумінні. Зміст кіберстійкості полягає у подвійній спрямованості. З одного боку, це включає операції із зміцнення протидії постійним кібератакам, забезпечення безперервності бізнесу в умовах, які можна вважати "нормальними" в умовах кібервійни, а з іншого боку кіберстійкість означає мінімізувати масштаби інцидентів кібербезпеки або запобігання втраті даних.

На виконання встановлених нормативних вимог Європейський центральний банк (ЄЦБ) планує протягом 2024 року провести перші стрес-тести на кіберстійкість, щоб визначити, наскільки добре окремі банки зможуть реагувати на кібератаки та відновлюватися після них. Стрес-тести включатимуть участь 109 банків, які перебувають під наглядом ЄЦБ та будуть зосереджені на тому, як банки реагують на кібератаки та відновлюють свою операційну діяльність, а не на їхній здатності запобігати їм. При цьому, 28 банків пройдуть розширену оцінку, для якої вони нададуть додаткову інформацію про те, як вони впоралися із кібератакою. Ця вибірка охоплює різні бізнес-моделі та географічні регіони, щоб забезпечити змістовне відображення банківської системи Єврозони. Планується, що отримані дані будуть використані для оприлюднення та подальшої наглядової оцінки у 2024 році [17].

Висновки.

ЄС робить важливі кроки з метою удосконалення власного законодавства щодо посилення кіберстійкості в умовах масштабних посягань у кібердомені, глобальних викликів та кіберзагроз, переважно російського походження. Згідно європейського законодавства загальноприйнятим визначенням кіберстійкості є здатність систем захищатися від інцидентів кібератак та підтримувати належний рівень продуктивності за рахунок підтримання критичної функціональності та своєчасного поновлення до рівня, який існував до кіберінцидента. Тобто – це здатність організації працювати в умовах кібератаки або кіберінциденту, яка передбачає наявність та використання технічних та організаційних заходів для виявлення, реагування та поновлення після подібних інцидентів, можливість адаптуватися до динамічних змін та підвищувати стійкість у майбутньому.

На теренах ЄС кіберстійкість особливо актуальна у питаннях забезпечення кібербезпеки, а умовною її мірою є адаптивна здатність та спроможність реагувати на загрозу, підтримувати належну функціональність систем з метою її стабільної роботи, максимального зниження ризиків кібербезпеки, запобігання тяжким наслідкам від кібератак. Таким чином, цілком логічно враховувати ймовірні ризики для кібербезпеки, які надають змогу оцінити вірогідність настання події та її наслідки, які можуть виникнути на випадок скоєння кібератак.

Важливою законодавчою вимогою встановлено підвищення обізнаності про важливість безпеки в цифрових продуктах, посилення відповідальності розробників програмного забезпечення, запровадження систем звітності та попередження про вразливості, щоб споживачі могли повідомляти про них, бачити статус безпеки та оновлень програмного забезпечення для пристроїв і бути попередженими про будь-які ризики.

Також висувається нормативна вимога, щоб виробники повідомляли Агентство Європейського Союзу з кібербезпеки (ENISA) про будь-які вразливості протягом 24 годин після їхнього виявлення. Ці вимоги призначені для захисту даних споживачів, але вони також дозволять виробникам уникнути глобальних порушень.

Основними цілями практичної реалізації положень Закону ЄС про кіберстійкість мають стати: суттєве зменшення вразливостей; посилення відповідальності за кібербезпеку для розробників та виробників програмних продуктів; підвищення прозорості на цифрових ринках. За таких умов задекларовано, що кібербезпека має стати важливою частиною кожного кроку життєвого циклу розробки пристрою чи програмного забезпечення; створюється протокол обліку ризиків, які мають бути задокументовані; виробники повинні повідомляти, обробляти та виправляти вразливості для будь-яких пристроїв, які реалізуються протягом очікуваного терміну служби продукту або протягом п’яти років, залежно від того, що станеться раніше; розробник або виробник повинен надавати чіткі та зрозумілі інструкції для будь-яких продуктів з цифровими елементами та нести відповідальність за дефекти та уразливості. Закон ЄС про кіберстійкість є результатом тривалих зусиль керівних органів ЄС з метою забезпечення більш глибокого рівня кібербезпеки. Ця спроба значною мірою є відповіддю на помітне збільшення кількості програм-вимагачів і кібератак особливо після початку війни рф проти України. Тим не менш, цей Закон узгоджений із деякими іншими стандартами, включаючи Директиву NIS2, яка являє собою загальне законодавство ЄС щодо кібербезпеки.

Враховуючи позитивний європейський досвід правового регулювання кіберстійкості, для України актуальною залишається імплементація положень

законодавства ЄС, присвяченого цій проблематиці, у національне законодавство. В сучасних умовах Україна, реагуючи на сучасні виклики та загрози, формує нові прагматичні підходи до посилення кіберстійкості в масштабах країни. В умовах тривалої російської війни проти України, у тому числі й у кібердомені, одним із найважливіших завдань є забезпечення кіберстійкості об'єктів критичної інформаційної інфраструктури, державних інформаційних ресурсів, комунікаційних та технологічних систем, що забезпечують функціонування органів державної влади в умовах правового режиму воєнного стану. Важливо забезпечити загальні правила обміну інформацією та налагодити взаємодовіру між усіма суб`єктами забезпечення кібербезпеки в умовах правового режиму воєнного стану, використовувати єдину таксономію кіберінцидентів та шкалу для вимірювання їхньої критичності, впровадити загальний підхід до реагування на кіберінциденти, в основі якого має перебувати екосистема культури кібербезпеки та захищені передові сучасні технології.

За таких умов існує нагальна потреба у законодавчому забезпеченні посилення спроможностей держави із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, що вимагає прискорення схвалення законопроекту "Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури" від 29.08.22 р. № 8087 [18]. Практичне впровадження положень цього законопроекту сприятиме створенню належної правової основи щодо стримування збройної агресії російської федерації у кіберпросторі та надання відсічі агресору.

Використана література

1. Cybercrime Index" Ranks: Russia, Ukraine, and China at the Top. URL: https://cybersecurity news.com/cybercrime-index-ranks

2. Гуржій С.В. Засади інституційно-функціонального забезпечення кібербезпеки в сучасних умовах. *Інформація і право.* № 2(37)/2021. С. 103-114. URL: DOI: 10.37750/2616-6798. 2021.2(37).238344.

3. Костроміна М.О., Гарнатко Л.О. Кіберстійкість і кібербезпека: у чому різниця? *Сучасний захист інформації.* 2022. № 4 (52). С. 71-75. DOI: 10.31673/2409-7292.2022.040 012.

4. Користін О.Є., Демедюк С.В.Актуалізація кіберстійкості та історичні витоки концепції "стійкість". *Аналітично-порівняльне правознавство.* 2023. № 6. С. 708-713. DOI 10.24144/ 2788-6018.2023.06.122.

5. Komarov M., Honchar S., Dimitriieva, D. (2021). Дослідження проблеми кіберживучості об'єктів критичної інформаційної інфраструктури. *Ядерна та радіаційна безпека*, № 1(89). С. 59-66. URL: https://doi.org/10.32918/nrs.2021.1(89).07

6. Maltseva I., Chernysh Y., Ovsiannikov, V. (2021). Аналіз методик оцінки кіберстійкості критичної інфраструктури. *Кібербезпека: освіта, наука, техніка.* № 4(12). С. 29-35. – (Електронне фахове наукове видання). URL: https://doi.org/10.28925/2663-4023.2021.12.2935

7. Шиповський В. Система показників оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури. *Захист інформації.* 2023. Т. 25. № 1. С. 37-45. DOI: 10.18 372/2410-7840.25.17597.

8. Autolitana, Simona. (2020). A Europe Fit for the Digital Age: The Quest for Cybersecurity Unpacked.*Istituto Affari Internationali Commentaries.* 1-6 p. URL: https://www.iai.it/en/pubblicazio ni/europe-fit-digital-age-quest-cybersecurity-unpacked

9. Cerulus, Laurens. (2020). EU bolsters defenses against cyberattacks**:** new strategy and laws aim to stop hacks of key assets and information. *Politico.* URL: https://www.politico.eu/article/eu-bolsters-defenses-against-cyberattacks/?fbclid=IwAR

10. Björck, F., Henkel, M., Stirna, J., Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol 353. Springer, Cham. URL: https://doi.org/10.1007/978-3-319-16486-1_31

11. AraujoM.S., Machado B.A., PasossF.U. Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. *Applied Sciences* 2024. URL: https://doi.org/10.3390/app14052116

12. Кіберстійкість: як досвід ЄС може допомогти Україні. URL: https://www.eurointegration.com.ua/articles/2021/06/11/7124258

13. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

14. Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive#:~:text=The%20Directive%20on%20measures%20for,them%20to%20be%20appropriately%20equipped

15. The Cyber Resilience Act (CRA) 15.09.2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

16. What is cyber resilience and what are the benefits? URL: https://www.future-processing.com/blog/what-is-cyber-resilience-and-what-are-the-benefits

17. ECB to stress test banks' ability to recover from cyberattack. URL: https://www. bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240103~a26e1930b0.en.html

18. Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури: проект закону України від 29.09.22 р. № 8087 URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40553

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~