УДК 004.056

Демедюк Сергій Васильович,
кандидат юридичних наук,
заступник Секретаря Ради національної
безпеки і оборони України,
м. Київ, Україна
ORCID ID 0009-0008-1359-5265

ІНСТИТУЦІОНАЛІЗАЦІЯ КІБЕРСТІЙКОСТІ

Статтю присвячено аналізу проблемних питань щодо розбудови кіберстійкості як здатності протистояти кіберризиками, відновлюватися та адаптуватися до них. Проаналізовано три типи інституційних підходів, які використовуються для підвищення кіберстійкості, що передбачає розроблення широкого спектру інструментів та заходів: маркетингового, що просувається індустрією кібербезпеки; стандартизованого, який намагаються упроваджувати у розроблюваних міжнародних стандартах кібербезпеки; і регуляторного на основі комплаєнсу та дотримання вимог, спрямованих на підвищення кіберстійкості.

Ключові слова: *кібербезпека, кіберризик, управління ризиками, кіберстійкість, стандарт, регуляторні органи.*

Витонченість та зростаючі частота й інтенсивність кібератак, спрямованих на установи у кіберпросторі, підкреслюють їх високу ризиковість та складність повноти захисту цілісності критично важливих об'єктів та систем. У цьому контексті кіберстійкість пропонує привабливу додаткову альтернативу існуючій парадигмі кібербезпеки. Загалом кіберстійкість визначається як здатність протистояти зовнішнім потрясінням, спричиненим кіберризиками, відновлюватися після них та адаптуватися до них. Водночас запити сучасного суспільства щодо поширення кіберстійкості потребують конкретизації заходів, методів та інструментів, що вирішують такого роду завдання.

Метою цієї статті є дослідження проблематики кіберстійкості та вивчення галузевих заходів, які сприяють, підтримують або санкціонують кіберстійкість, а також викликів, з якими вони стикаються.

Кіберстійкість останнім часом стала однією з найбільш розкручених концепцій у дискусіях про кібербезпеку. Зокрема, виділяється три типи інституційних підходів, що забезпечують певні галузеві заходи кіберстійкості [1]: маркетинг, стандартизація та регулювання. Кожен підхід реалізується певною групою інституцій, які переслідують різні цілі і можуть використовувати широкий набір ресурсів, які варіюються від простого переконання та стимулювання до примусу. Кожна з цих груп має своє розуміння кіберстійкості та шляхів її досягнення.

Маркетинг кіберстійкості. Протягом 2013–2018 років кіберстійкість стала основною темою в постійному потоці звітів, що випускаються процвітаючою індустрією кібербезпеки. Щонайменше 11 компаній, що продають консалтингові послуги (Accenture,

EY, McKinsey, PwC), сертифікацію найкращих практик (Axelos), страхування (AIG), програмне та апаратне забезпечення для забезпечення безпеки (Cisco, IBM, Symantec, UpGuard) або послуги з управління безпекою (SecureWorks) випустили маркетингові матеріали, які визначають переваги кіберстійкості та знайомлять наявних або потенційних клієнтів з тим, що, на їхню думку, є майбутнім кібербезпеки. Одна компанія навіть заявила, що «кібербезпека померла», наводячи переконливі аргументи на користь кіберстійкості як єдиної життєздатної моделі, що залишилася [2].

Для кращого розуміння інструментальної природи концепції кіберстійкості та неоднорідності її значення в індустрії кібербезпеки було узагальнено звіти цих компаній та визначено концептуальні елементи, притаманні кіберстійкості [1].

Незважаючи на активну пропаганду, менше половини (4 з 11) проаналізованих звітів надали визначення того, що таке кіберстійкість. Хоча більшість цих визначень містять звичайні посилання на підготовку, виявлення, реагування на інциденти та пом'якшення наслідків, деякі з них були більш загадковими і межували з грандіозними, як, наприклад, визначення UpGuard: «Кіберстійкість – це спосіб використання технологій на підприємстві для досягнення успіху» [2]. Сім звітів, які не надають робочого визначення, припускають, що концепція кіберстійкості є самозрозумілою або інтуїтивно зрозумілою для фахівців-практиків. Таким чином, кіберстійкість визначається не стільки тим, чим вона є, скільки тим, що вона прагне замінити застарілу модель традиційної кібербезпеки, яка не здатна впоратися зі складним і руйнівним характером кіберризиків. У жодному з 11 розглянутих звітів не міститься жодного посилання на більш загальну концепцію стійкості в таких галузях, як інженерія, управління катастрофами, управління соціально-екологічними системами або психологія, що ілюструє вузькість їхньої сфери застосування.

Хоча визначення кіберстійкості є нечітким, перераховано широкий спектр складових технологій, процесів і практик, які демонструють зростання організаційної спроможності в цій сфері. У 11 звітах було виявлено дванадцять елементів кіберстійкості, перелічених у порядку зменшення частоти: спільна відповідальність (10), виявлення загрози (9), реагування на інциденти (9), запобігання (8), мапування ризиків (7), відновлення (6), мережевий потенціал (6), розробка кризових сценаріїв (5), моделювання (5), адаптація (5), цифрова криміналістика (2) і страхування (1).

Поняття спільної відповідальності, яке згадується найчастіше, стосується необхідності залучення більш широкого кола структурних підрозділів (разом з керівниками) до запобігання та пом'якшення кіберризиків, ніж це зазвичай має місце в більш традиційних підходах до кібербезпеки (визначення відповідальним директора з інформаційної безпеки (*Chief information security officers (CISO)*).

Наступні три функції є більш технічно орієнтованими на контроль, виявлення та реагування на кіберінциденти. Цікаво відзначити, що більш запобіжного характеру заходи, такі як мапування ризиків, розробка кризових сценаріїв і моделювання інцидентів, а також заходи, спрямовані на відновлення, співпрацю з третіми сторонами та адаптацію, рекомендуються більш епізодично. Трансформаційний потенціал кіберстійкості згадується лише двічі [2; 3], можливо, тому, що 11 досліджуваних компаній не пропонують

конкретних продуктів і послуг для підтримки цієї більш розрізненої діяльності. Нарешті, такі особливі заходи, як цифрова криміналістика та кіберстрахування, пропонуються лише компаніями, які працюють у цих конкретних сегментах ринку кібербезпеки.

Разом з тим, у зазначених звітах прослідковується прямий зв'язок між пропагованими шляхами до кіберстійкості та продуктами і послугами, які пропонують корпоративні спонсори цих звітів. Зокрема, документ компанії Symantec закінчується зверненням до читача *«зв'язатися з представником Symantec, щоб обговорити, як можна почати впроваджувати кіберстійкість у стратегію безпеки»* [4], звіт Cisco наголошує, як її технічні продукти можуть бути використані для підвищення стійкості мережевої архітектури [5], а UpGuard розкидає скріншоти своєї платформи CSTAR у своєму звіті, щоб проілюструвати, як вона може допомогти клієнтам реалізувати конкретні цілі кіберстійкості (за визначенням компанії).

Зазначене свідчить насамперед про упередженість та обмеженість поглядів на кіберстійкість, на які значною мірою впливають інтереси їхніх спонсорів, а їхній внесок у загальну скарбничку знань про кіберстійкість залишається досить скромним.

Проте мають місце і більш глибокі та системні підходи. Існує кілька винятків: звіти PwC та Accenture включають результати опитувань, проведених серед 9 500 та 4 600 міжнародних керівників відповідно [3; 6], тоді як IBM замовляє щорічне дослідження кіберстійкості від Ponemon Institute [7]. Незважаючи на ці нечисленні спроби розробити більш систематизовану базу знань про поширеності практик кіберстійкості в організаціях, більшість галузевих звітів залишаються нормативними, не розкриваючи доказів, що підтверджують їхні приписи. У цьому відношенні деякі звіти майже копіюють межі кіберстійкості, розроблені організаціями зі стандартизації.

Стандартизація кіберстійкості. Стандарт можна визначити як правило або норму, яку можна виміряти, випробувати, дослідити і переглянути, а іноді його описують як «рецепт реальності» [8]. Стандарти застосовуються до продуктів, процесів або людей і стали повсюдними у складному світі, де потоки товарів, інформації, грошей і людей мають бути скоординовані та синхронізовані в глобальному масштабі. Стандарти, хоча часто невидимі, підтримують технічну та організаційну інфраструктуру, які уможливлюють сучасне життя [9; 10]. Тому вони відіграють центральну роль в управлінні ризиками, допомагаючи зменшити невизначеність та інформаційну асиметрію, які ускладнюють взаємодію між партнерами. Навіть необов'язкові стандарти, які здаються несуттєвими і нейтральними, мають велику силу, оскільки вони контролюють «можливість встановлювати правила, яких дотримуються інші, або встановлювати перелік критеріїв, з якого вони можуть обирати» [8]. Поширення стандартів було прискорене зростанням кількості національних і міжнародних органів, що встановлюють стандарти органів, які об'єднують державні та галузеві зацікавлені сторони [11].

У сфері кібербезпеки домінують два загальні стандарти, які включають заходи, сумісні з підходом до кіберстійкості: стандарти Міжнародної організації зі стандартизації (*International Organization for Standardization (ISO)*) 27000-серії щодо стандартів інформаційної безпеки та Національного інституту стандартів і технологій (*National Institute of Standards and Technology (NIST)*).

Міжнародна організація зі стандартизації (ISO) базується у Швейцарії та об'єднує 163 національні органи стандартизації. З моменту свого створення у 1947 році вона розробила понад 22 000 стандартів. У співпраці з Міжнародною електротехнічною комісією (*International Electrotechnical Commission (IEC)*) вона підтримує набір із понад 40 стандартів інформаційної безпеки, які охоплюють широкий спектр питань – від створення спільної термінології до розробки та впровадження засобів контролю управління ризиками й найкращих практик реагування на інциденти до судових розслідувань [12]. Це сімейство стандартів бере свій початок із більш ранньої роботи Британського інституту стандартів, який прийняв кодекс практики управління інформаційною безпекою у 1995 році. Згодом цей стандарт був гармонізований ISO і привів до створення стандарту ISO/IEC 27001 у 2005 році, за яким послідували 39 більш спеціалізованих, але все ще взаємопов'язаних стандартів [13]. Стандарт ISO/IEC 27001 побудований навколо восьми функцій високого рівня, які варіюються від розуміння «контексту організації» до «лідерства», «планування», «підтримки», «документування інформації», «функціонування», «оцінювання результативності» та «вдосконалення». Зазначені пункти розбиті на 35 цілей і 114 засобів контролю (або заходів), які відповідають вимогам цього стандарту. Складність цієї структури ускладнюється тим, що ці заходи не представлені та не обговорюються в порядку пріоритетності впровадження, що може зробити їх імплементацію непосильним завданням навіть для організації, яка бажає їх запровадити. Станом на 2017 рік було видано понад 39 000 чинних сертифікатів організаціям, які продемонстрували свою відповідність стандарту, але половина з них була сконцентрована в п'яти країнах (Японія, Великобританія, Індія, Китай, Німеччина), що ілюструє постійний низький рівень та нерівномірність прийняття стандарту у порівнянні з набагато більш успішною серією стандартів ISO 9000 [14].

Хоча сімейство стандартів серії 27000 явно не включає стійкість як одну зі своїх цілей, вона рекомендує багато заходів, які сприяють кіберстійкості організації, такі як «обізнаність, освіта та навчання з питань інформаційної безпеки», «резервне копіювання інформації», «планування безперервності інформаційної безпеки» або «навчання на основі інцидентів інформаційної безпеки», і це лише деякі з них. Комітет, відповідальний за розробку цього сімейства стандартів (відомий як ISO/IEC JTC 1/SC 27), також регулярно підтримує зв'язок з Комітетом ISO з питань стійкості (ISO/TC 292, який відповідає за стандарт ISO 22316) стандарт організаційної стійкості ISO 22316, оновлений у 2017 році), а також з комітетом з управління ризиками та безпеки (ISO/TC 262). Більш сфокусований стандарт (ISO/IEC 27035) містить набір настанов щодо планування, підготовки та проведення заходів із реагування на кіберінциденти. Відповідність цьому стандарту дає організаціям можливість протистояти неочікуваним та невідомим загрозам, а його п'ять етапів відображають динамічну природу кіберстійкості: планування та підготовка, виявлення та інформування, оцінка та прийняття рішень, реагування та засвоєння уроків [15]. Її більш детальні заходи також підкреслюють мережеві, практичні та адаптивні виміри стійкості.

Другий стандарт кібербезпеки, який привернув великий міжнародний інтерес, незважаючи на своє національне походження, розроблений у США Національним інсти-

тутом стандартів і технологій (NIST). Створений у 1901 році NIST описує себе як нерегулятивне федеральне агентство, яке надає технології, вимірювання та стандарти для промисловості США з метою підвищення їхньої конкурентоспроможності.

Кібербезпека – це добровільний інструмент, спочатку розроблений за вказівкою Білого дому і запущений у 2014 році з метою покращення цифрової безпеки критично важливої інфраструктури [16]. Рамкова концепція кібербезпеки, що з'явилася в результаті тривалих консультацій з широким колом зацікавлених сторін у промисловості, уряді та академічних колах, має на меті консолідувати наявні стандарти та практики, а також виявити прогалини, для усунення яких необхідні оновлені або нові стандарти [17]. На відміну від свого аналога ISO, який має бути придбаний компаніями і надає сертифікат відповідності, що видається акредитованою третьою стороною, Рамка кібербезпеки NIST є безкоштовною і не підтримується формальним процесом оцінки відповідності, а це означає, що її впровадження залишається пристосованим до індивідуальних потреб і можливостей кожної організації, що приймає її.

Рамкова програма NIST організована навколо «ядра» з п'яти функцій (ідентифікація, захист, виявлення, реагування та відновлення), які зі свого боку поділяються на 23 категорії цілей і 108 підкатегорій результатів. Кожен результат співвідноситься з аналогічними заходами або засобами контролю, що містяться в інших стандартах кібербезпеки, таких як ISO/IEC 27001 або COBIT 5.

Визнаючи, що організації значно відрізняються за своєю здатністю впроваджувати Рамкову програму, передбачено чотири «рівні впровадження»: частковий, з урахуванням ризиків, повторюваний та адаптивний [18; 19]. Кожен рівень фіксує прогрес у ступені кіберстійкості до більш цілісного, адаптивного та мережевого потенціалу. Бібліотека публікацій, організована за функціями, каталог історій успіху та щорічна конференція доступні для підтримки користувачів Рамкової програми у їхніх зусиллях з імплементації. Значна кількість категорій та підкатегорій де-факто орієнтовані на кіберстійкість (наприклад, тестування планів реагування та відновлення, впровадження механізмів для досягнення технічної стійкості в нормальних і несприятливих ситуаціях, пом'якшення наслідків інцидентів та включення отриманих уроків до планів відновлення), але, як і в стандарті ISO/IEC, немає чіткого розмежування між кібербезпекою та кіберстійкістю, а також не визначено пріоритетів чи ранжування заходів, щоб вказати ті з них, які є найбільш важливими, на відміну від тих, що є другорядними або повинні розглядатися лише найбільш зрілими адептами [20].

У березні 2018 року NIST опублікував проєкт документа, в якому викладено набір керівних принципів і просить надати коментарі щодо того, як слід розробляти кіберстійкі системи [21]. Ця публікація, не пов'язана з Рамковою концепцією кібербезпеки, використовує суто технічний підхід, який менше стосується загальної стійкості організацій, що стикаються з кібершоком, ніж живучості їхніх цифрових активів. Незважаючи на вужчу спрямованість, цей майбутній стандарт чітко узгоджує свої принципи побудови з чотирма цілями кіберстійкості – передбачення, протистояння, відновлення та адаптація, а також з більш конкретним набором з 8 цілей і 14 методів, мотивованих попередніми дослідженнями, проведеними на початку 2010-х років у MITRE Corporation [21; 22].

Виходячи за межі загальних стандартів кібербезпеки, запроваджених ISO/IEC і NIST, були запропоновані більш спеціалізовані стандарти щодо різних етапів і сфер кіберстійкості. Найбільш детальним з них є Модель управління стійкістю CERT (CERT-RMM), розроблена підрозділом Інституту інженерії програмного забезпечення Університету Карнегі-Меллона [23]. Цей 860-сторінковий документ надає всеосяжну структуру операційної стійкості, що є результатом формалізації та консолідації найкращих практик на стику IT-безпеки, безперервності бізнесу та реагування на катастрофи. CERT-RMM прагне знайти шляхи для декомпозиції та інституціоналізації кіберстійкості, а також визначити правильний баланс між технічними та організаційними заходами, необхідними для її посилення, наголошуючи на необхідності підтримування високого рівня контекстуальної та ситуативної обізнаності, розвитку мережевих та відпрацьованих навичок управління загрозами та посилення адаптивних можливостей. Вона організована навколо 26 сегментів процесу, які розбиті на 94 конкретні цілі і 256 конкретних практик. Як і в NIST, можливим є відображення у форматі детальної таблиці перехресних посилань певних відповідностей і прогалин з іншими стандартами, такими як ISO/IEC, COBIT та багатьма іншими практиками. Розроблений на цій основі інструмент самооцінки, який більше зосереджений на кіберризиках і сумісний із NIST, доступний задля допомогти організаціям в оцінюванні власного рівня кіберстійкості [24].

Водночас Агентство Європейського Союзу з мережевої та інформаційної безпеки (*European Union Agency for Network and Information Security (ENISA)*) з 2009 року здійснює моніторинг та доповнює роботу органів стандартизації у сфері кібербезпеки, де кіберстійкість є особливою сферою інтересів [25]. У 2009 році видано посібник з передової практики щодо розробки, проведення та оцінки національних навчань із підвищення кіберстійкості публічних комунікаційних мереж [26]. У 2011 році опубліковано технічний звіт, у якому було розглянуто наявні системи вимірювання та метрики для стійких мереж і послуг і, нарікаючи на відсутність стандартизованої системи, запропоновано уніфіковану таксономію для використання організаціями [27]. Агенцією також розроблена онлайн-платформа, яка підтримує роботу експертних груп, що розробляють галузеві настанови з кіберстійкості.

Всесвітній економічний форум (*The World Economic Forum*), хоча технічно не є органом зі стандартизації, також визначив кіберстійкість одним зі своїх пріоритетних питань, що відображає зростання кіберризиків як однієї з двох основних проблем, що турбують його членів (поряд з екологічними ризиками) [28]. У відповідь на це розроблено систему кіберстійкості для рад директорів, яка містить набір з 10 принципів і 47 детальних питань, що представляють елементи або заходи, які, як вважається, посилюють управління діяльністю з кіберстійкості у цій сфері [29].

Усі розглянуті вище добровільні стандарти як загальні, так і спеціалізовані, мають спільне базове припущення: вони неявно припускають, що кіберстійкість може бути досягнута майже механічно, шляхом трудомісткого впровадження довгого переліку надмірно деталізованих технічних та організаційних заходів контролю. У цій домінуючій моделі, мотивованій інженерним мисленням, здатність поглинати, протистояти і адаптуватися до кібершоків розглядається як результат кумулятивного і стабільного

процесу, в якому заходи, хоч і вважаються однаковим внеском у кінцевий результат, все ж не представляються у певному порядку важливості. При такому підході втрачається непередбачуваний, несподіваний і дестабілізуючий характер кіберкриз і необхідність розвитку загальних ресурсів та спроможностей, які можуть адаптуватися і вистояти.

Регулювання кіберстійкості. Зростаюча ймовірність і серйозність кіберризиків, що впливають на різні установи і здатні дестабілізувати цілі системи (фінансові, енергетичні, телекомунікаційні тощо), підштовхнуло регуляторні органи до розробки широкого спектру заходів з оцінки та комплаєнсу, з метою посилення кіберстійкості установ, за якими вони здійснюють нагляд. У питаннях регулювання кіберстійкості визнається, що не всі організації бажають або можуть добровільно прийняти стандарти і практики, які покращать їхню здатність витримувати кібершок. Однак, враховуючи гіперзв'язане та взаємозалежне середовище, в якому працюють ці організації, такий брак занепокоєння та бездіяльності може стати джерелом спільних втрат. Тому деякі регулятори вивчають низку стратегій, що охоплюють повний спектр піраміди комплаєнсу – від підвищення обізнаності та освіти до більш жорстких форм взаємодії та правозастосування. Ідея піраміди комплаєнсу запозичена з роботи Айреса та Брейтуейта [30], з її основним принципом «безпечної великої гармати», який полягає в тому, що ескалація правозастосовної практики повинна розглядатися як спосіб індивідуалізації інтенсивності регуляторної діяльності відповідно до поведінки окремих суб'єктів. Стратегією у цьому контексті є неінтрузивне та делеговане регулювання, яке з більшою ймовірністю сприятиме співпраці між приватними суб'єктами, оскільки дозволяє їм на власний розсуд вирішувати, як найкраще досягти регуляторних цілей, зокрема підвищення кіберстійкості. Маючи справу з приватними суб'єктами, які не бажають або не можуть впроваджувати ефективні стратегії, держава зберігає можливість ескалації свого втручання, переходу до адміністративних методів регулювання, які передбачають різні форми впливу. Ця теорія глибоко вкорінена в стратегії відповідальності, описаній Гарландом, згідно з якою державні органи *«формують стратегічні відносини з іншими силами соціального контролю [...] для створення широких альянсів, залучаючи повноваження приватних суб'єктів і формуючи їх відповідно до цілей контролю ...»* [31]. Але загальна стратегія є більш широкого діапазону, і не покладаючись виключно на механізми покарання і примусу, як це пропонує Гарланд, натомість розглядає більш повний перелік методів втручання, які включають переконання та медіацію [32]. У цьому відношенні притягнення до відповідальності відбувається як добровільно, з власних інтересів, так і в результаті регуляторної діяльності держави.

Подібно до маркетингового підходу та підходу стандартизації, регуляторному підходу все ще бракує концептуальної ясності на цьому ранньому етапі його використання [1]. Деякі регуляторні органи використовують терміни «кібербезпека» та «кіберстійкість» як взаємозамінні, що не допомагає суб'єктам регулювання зрозуміти нюанси та взаємодоповнюваність обох підходів.

Таким чином, ураховуючи зазначені підходи щодо забезпечення кіберстійкості, очевидним є те, що різноманітна теоретична та нормативна література потребує доповнення переконливими емпіричними даними про те, які організаційні властивості та

заходи сприяють або перешкоджають кіберстійкості. Ці зусилля мають бути спрямовані не лише на вибірку тематичних досліджень, які можуть слугувати уроками з кіберстійкості, а й покращувати здатність вимірювати прогрес кіберстійкості на практиці. Показники кіберстійкості залишаються недостатньо дослідженими, і слід розпочинати спільні зусилля за участю практиків та науковців, щоб забезпечити наявність правильних інструменти для вимірювання того, що має значення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Benoit Dupont.* The cyber-resilience of financial institutions: significance and applicability. Journal of Cybersecurity. 2019. Vol. 5, № 1. С. 1-17. URL: https://doi: 10.1093/cybsec/tyz013 (дата звернення: 12.09.2023).

2. UpGuard. Cyber Resilience for the C-Suite. Mountain View: UpGuard, 2017.

3. PwC. Strengthening Digital Society against Cyber Shocks. London: PwC, 2018.

4. Symantec. The Cyber Resilience Blueprint: A New Perspective on Security. Mountain View: Symantec, 2015.

5. Cisco. Cyber Resilience: Safeguarding the Digital Organization. San Jose: Cisco, 2016.

6. Accenture. Gaining Ground on the Cyber Attacker: 2018 State of Cyber Resilience. Dublin: Accenture, 2018.

7. The Third Annual Study on the Cyber Resilient Organization. Traverse City: Ponemon Institute, 2018.

8. *Busch L.* Standards: Recipes for Reality. Cambridge: The MIT Press, 2011.

9. Standards and Their Stories. How Quantifying, Classifying, and Formalizing Practices Shape Everyday Life / Edited by M. Lampland, S. Leigh Star. Ithaca & London: Cornell University Press, 2009.

10. *Gorur R.* The invisible infrastructure of standards. Critical Studies in Education. 2013. Vol. 54, Iss. 2. P. 132–42.

11. *Brunsson N., Jacobsson B. A* World of Standards. Oxford: Oxford University Press, 2000.

12. *Lewis B.* How to tackle today's IT security risks. ISOfocus. 2019. Vol. 132. P. 6–11.

13. *Disterer G.* ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security. 2013. Vol. 4. P. 92–100.

14. *Fomin V., Vries H., Barlette Y.* ISO/IEC 27001 Information systems security management standard: Exploring the reasons for low adoption. EuroMOT 2008 - The Third European Conference on Management of Technology, Nice, France. September 2008. URL: https://www.researchgate.net/publication/228898807_ISOIEC_27001_Information_Systems_Security_Management_Standard_Exploring_the_reasons_for_low_adoption (дата звернення: 12.09.2023).

15. ISO/IEC. ISO/IEC 27035-1: Information Technology – Security Techniques – Information Security Incident Management – Part 1: Principles of Incident Management. Geneva: ISO, 2016.

16. NIST. History and creation of the framework. URL: https://www.nist.gov/ cyberframework/online-learning/history-and-creation-framework. (дата звернення: 12.09.2023).

17. NIST. Framework for Improving Critical Infrastructure Cybersecurity. Washington DC: NIST, 2014.

18. *Lei S.* The NIST Cybersecurity Framework: overview and potential impacts. SciTech Lawyer. 2014. Vol. 10. P. 16–19.

19. *Schackelford S., Proia A., Martell B.,* et al. Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices. Texas International Law Journal. 2015. Vol. 50. P. 305–355.

20. *Collier Z., DiMase D., Walters S.,* et al. Cybersecurity standards: managing risk and creating resilience. Computer. 2014. Vol. 47. P. 70–76. URL: https://doi: 10.1109/MC.2013.448 (дата звернення: 12.09.2023).

21. *Ross R., Graubart R., Bodeau D.,* et al. Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. Washington DC: NIST, 2018.

22. *Bodeau D., Graubart R.* Cyber Resiliency Engineering Framework. Bedford: The MITRE Corporation, 2011.

23. *Caralli R., Allen J., White D.,* et al. CERT Resilience Management Model, Version 1.2. Pittsburgh: Carnegie Mellon University, 2016.

24. DHS. Cyber Resilience Review (CRR): Self-Assessment Package. Washington DC: Department of Homeland Security, 2016.

25. *Purser S.* Standards for cyber security. In: Hathaway M. (ed.). Best Practices in Computer Network Defense: Incident Detection and Response. Amsterdam: IOS Press, 2014. P. 97–106.

26. ENISA. Good Practice Guide on National Exercises: Enhancing the Resilience of Public Communications Networks. Heraklion: ENISA, 2009.

27. ENISA. Resilience Metrics and Measurements: Technical Report. Heraklion: ENISA, 2011.

28. WEF. The Global Risks Report 2019, 14th Edition. Geneva: World Economic Forum, 2019.

29. WEF. Advancing Cyber Resilience: Principles and Tools for Boards. Geneva: World Economic Forum, 2017.

30. *Ayres I., Braithwaite J.* Responsive Regulation. New York: Oxford University Press, 1992.

31. *Garland D.* The Culture of Control: Crime and Social Order in Contemporary Society. Chicago: The University of Chicago Press, 2001.

32. *Braithwaite J.* What's wrong with the sociology of punishment? Theoretical Criminology. 2003. Vol. 7. P. 5–28. URL: https://doi.org/10.1177/1362480603007001198 (дата звернення: 12.09.2023).

REFERENCES

1. *Benoit, Dupont* (2019). The cyber-resilience of financial institutions: significance and applicability, Journal of Cybersecurity, 5:1, 1-17. URL: https://doi: 10.1093/cybsec/tyz013. (Date of Application: 12.09.2023) [in English].

2. UpGuard (2017). Cyber Resilience for the C-Suite. Mountain View: UpGuard [in English].

3. PwC (2018). Strengthening Digital Society against Cyber Shocks. London: PwC [in English].

4. Symantec (2015). The Cyber Resilience Blueprint: A New Perspective on Security. Mountain View: Symantec [in English].

5. Cisco (2016). Cyber Resilience: Safeguarding the Digital Organization. San Jose: Cisco [in English].

6. Accenture (2018). Gaining Ground on the Cyber Attacker: 2018 State of Cyber Resilience. Dublin: Accenture [in English].

7. The Third Annual Study on the Cyber Resilient Organization (2018). Traverse City: Ponemon Institute [in English].

8. *Busch, L.* (2011). Standards: Recipes for Reality. Cambridge: The MIT Press [in English].

9. Standards and Their Stories. How Quantifying, Classifying, and Formalizing Practices Shape Everyday Life / Edited by M. Lampland, S. Leigh Star. Ithaca & London: Cornell University Press, 2009 [in English].

10. *Gorur, R.* (2013). The invisible infrastructure of standards, Critical Studies in Education, 54:2, 132-42 [in English].

11. *Brunsson, N. & Jacobsson, B.* (2000). A World of Standards. Oxford: Oxford University Press [in English].

12. *Lewis, B.* (2019). How to tackle today's IT security risks, ISOfocus, 132, 6-11 [in English].

13. *Disterer, G.* (2013). ISO/IEC 27000, 27001 and 27002 for information security management, Journal of Information Security, 4, 92-100 [in English].

14. *Fomin, V., Vries, H. & Barlette, Y.* (September 2008). ISO/IEC 27001 Information systems security management standard: Exploring the reasons for low adoption. EuroMOT 2008 - The Third European Conference on Management of Technology, Nice, France. URL: https://www.researchgate.net/publication/228898807_ISOIEC_27001_Information_Systems_Security_Management_Standard_Exploring_the_reasons_for_low_adoption. (Date of Application: 12.09.2023) [in English].

15. ISO/IEC (2016). ISO/IEC 27035-1: Information Technology – Security Techniques – Information Security Incident Management – Part 1: Principles of Incident Management. Geneva: ISO [in English].

16. NIST. History and creation of the framework. URL: https://www.nist.gov/ cyberframework/online-learning/history-and-creation-framework. (Date of Application: 12.09.2023) [in English]

17. NIST (2014). Framework for Improving Critical Infrastructure Cybersecurity. Washington DC: NIST [in English].

18. *Lei, S.* (2014). The NIST Cybersecurity Framework: overview and potential impacts, SciTech Lawyer, 10, 16-19 [in English].

19. *Schackelford, S., Proia, A., Martell, B.,* et al. (2015). Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices, Texas International Law Journal, 50, 305-355 [in English].

20. *Collier, Z., DiMase, D., Walters, S.,* et al. (2014). Cybersecurity standards: managing risk and creating resilience, Computer, 47, 70-76. URL: https://doi:10.1109/MC.2013.448 (Date of Application: 12.09.2023) [in English].

21. *Ross, R., Graubart, R., Bodeau, D.,* et al. (2018). Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. Washington DC: NIST [in English].

22. *Bodeau, D. & Graubart, R.* (2011). Cyber Resiliency Engineering Framework. Bedford: The MITRE Corporation [in English].

23. *Caralli, R., Allen, J., White, D.,* et al. (2016). CERT Resilience Management Model, Version 1.2. Pittsburgh: Carnegie Mellon University [in English].

24. DHS (2016). Cyber Resilience Review (CRR): Self-Assessment Package. Washington DC: Department of Homeland Security [in English].

25. *Purser, S.* (2014). Standards for cyber security. In: Hathaway M. (ed.). Best Practices in Computer Network Defense: Incident Detection and Response. Amsterdam: IOS Press. P. 97-106 [in English].

26. ENISA (2009). Good Practice Guide on National Exercises: Enhancing the Resilience of Public Communications Networks. Heraklion: ENISA [in English].

27. ENISA (2011). Resilience Metrics and Measurements: Technical Report. Heraklion: ENISA [in English].

28. WEF (2019). The Global Risks Report 2019, 14th Edition. Geneva: World Economic Forum [in English].

29. WEF (2017). Advancing Cyber Resilience: Principles and Tools for Boards. Geneva: World Economic Forum [in English].

30. *Ayres, I. & Braithwaite, J.* (1992). Responsive Regulation. New York: Oxford University Press [in English].

31. *Garland, D.* (2001). The Culture of Control: Crime and Social Order in Contemporary Society. Chicago: The University of Chicago Press [in English].

32. *Braithwaite, J.* (2003). What's wrong with the sociology of punishment? Theoretical Criminology, 7, 5-28. URL: https://doi.org/10.1177/1362480603007001198. (Date of Application: 12.09.2023) [in English].

DOI (Issue): https://doi.org/10.36486/np.2023.4(62) Issue 4(62) 2023

UDC 004.056

Demediuk Serhii,
Candidate of Juridical Sciences (Ph.D),
Deputy Secretary of the National Security
and Defense Council of Ukraine,
Kyiv, Ukraine,
ORCID ID 0009-0008-1359-5265

INSTITUTIONALIZATION OF CYBER RESILIENCE

The article is devoted to the analysis of problematic issues related to the development of cyber resilience as the ability to withstand, recover from and adapt to cyber risks.

The author analyzes three types of institutional approaches used to enhance cyber resilience, which involves the development of a wide range of tools and measures: marketing, promoted by the cybersecurity industry; standardized, which is being implemented in the international cybersecurity standards being developed; and regulatory, based on compliance and enforcement aimed at enhancing cyber resilience.

It is noted that representatives of the cybersecurity industry define cyber resilience mainly through the desire to replace the outdated model of traditional cybersecurity, which is unable to cope with the complex and destructive nature of cyber risks. It is pointed out that the views on cyber resilience are biased and limited, heavily influenced by business interests, and that their contribution to the development of the cyber resilience knowledge system is insufficient.

It is emphasized that two general standards dominate the field of cybersecurity, which include measures that are compatible with the cyber resilience approach: the ISO 27000-series and NIST standards. Although ISO-27000 does not explicitly include resilience as one of its goals, it recommends many measures that contribute to an organization's cyber resilience, such as information security awareness, education and training, information backup, information security continuity planning or information security incident-based learning, etc. At the same time, the NIST Cybersecurity Framework is free of charge and is not supported by a formal compliance assessment process, which means that its implementation remains tailored to the individual needs and capabilities of each organization that adopts it. At the same time, a mechanistic approach to building cyber resilience based on standardization misses the need to develop common resources and capabilities that can adapt and withstand.

It is noted that the strategy of the regulatory approach is non-intrusive and delegated regulation, which is more likely to promote cooperation and best contribute to the regulatory goals of enhancing cyber resilience. At the same time, all marketing, standardization, and regulatory approaches are characterized by a lack of clear conceptual content of cyber resilience measures.

Keywords: cybersecurity, cyber risk, risk management, cyber resilience, standard, regulatory authorities.

Отримано 21.11.2023