element of corporate governance responsibility that defines a company's safety policy and its intentions to manage safety as an integral part of its overall business. Thus, the security management system (Security Management System, SeMS) is a part of the overall information asset management system of the aviation enterprise, which is based on risk analysis and is intended for the design, implementation, control, monitoring and improvement of measures in the field of information security. This system consists of organizational structures, policies, planning actions, responsibilities and procedures, processes and resources, and much more. An analysis of modern management measures of the information security system of air transport facilities based on international standards of the ISO series was carried out. A scenario for the implementation of the plan for managing the security of information assets of the air transport complex is proposed, which is based on the best experience of foreign countries.
Keywords: information security, risk level, air transport complex, policies, confidentiality, availability, integrity, terms of reference, security systems.

Шульга Володимир Петрович, доктор історичних наук, в.о. ректора Національного авіаційного університету, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
Volodymyr Shulha, Acting Rector of National Aviation University, professor of IT-Security Academic Department, National Aviation University.
E-mail: shulga.khnuvs@gmail.com.
Orcid ID: 0000-0003-4356-7288.

Міщенко Андрій Віталійович, доктор технічних наук, професор, професор кафедри засобів захисту інформації Національного авіаційного університету.

Andrii Mishchenko, doctor of technical science, professor, professor of the Department of information security National Aviation University.
E-mail: td@airport.kiev.ua.
Orcid ID: 0000-0001-8376-1777.

Моркляник Богдан Васильович, доктор технічних наук, професор, член Національного агенства кваліфікацій.

Bohdan Morklyanyk, doctor of technical science, professor, Member National Qualifications Agency.
E-mail: kzzi@nau.edu.ua.
Orcid ID: 0009-0000-6564-6804.

Лазаренко Сергій Володимирович, доктор технічних наук, професор, професор кафедри засобів захисту інформації Національного авіаційного університету.

Serhii Lazarenko, doctor of technical science, professor, professor of the Department of information security National Aviation University.
E-mail: zzi.lazarenko@nau.edu.ua.
Orcid ID: 0000-0003-3529-4806.

Ліщиновська Наталія Олександрівна, кандидат технічних наук, асистент кафедри засобів захисту інформації Національного авіаційного університету.

Natalia Lishchynovska, Ph.D., assistant of the Department of information security National Aviation University.
E-mail: natashalil858@ukr.net.
Orcid ID: 0000-0002-1913-8419.

DOI: 10.18372/2410-7840.25.18228
УДК 004.621.5

АНАЛІЗ ПОНЯТТЯ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Євгенія Іванченко, Олександр Корченко, Олег Зарицький, Сергій Зибін, Наталія Вишневська

У зв'язку зі збільшенням кількості кібератак та інцидентів на об'єкти критичної інфраструктури перед спеціалістами постає проблема підвищення ефективності заходів безпеки, які будуть в змозі забезпечити надійну та безперебійну роботу об'єктів критичної інфраструктури в цілому. Тому поняття кіберстійкість, управління кіберстійкістю, забезпечення кіберстійкості, оцінювання кіберстійкості набувають подальшої актуалізації. До поняття кіберстійкості, крім безпеки, відносять низку завдань і процесів, які стосуються інформаційних технологій (наприклад, резервування та відновлення після збоїв) і захисту бренду. Причому питання стійкості і безперервності сервісів в цьому понятті відносяться як до самої компанії, так і до зовнішніх підрядників, які надають такі послуги. Так, Держспецзв'язку визначили, що передумовою до появи кіберстійкості як напрямку корпоративної кібербезпеки стало прийняття компаніями факту про неминучість кібератаки. В поняття кіберстійкості також включають можливість підготуватися до атаки, забезпечення ефективної діяльності та протидії під час атаки, а також зниження можливих наслідків атаки на компанію. Важливим для підприємств є оцінювання стану кіберстійкості їх критичних інфраструктур для

планування вкладання коштів, що дозволяють забезпечити необхідний рівень кіберстійкості. Але для реалізації процесу оцінювання необхідно чітко розуміти, що стоїть за зазначеним поняттям. Тому актуальною задачею є аналіз поняття кіберстійкості критичної інфраструктури. Метою роботи є аналіз понять кіберстійкості для критичних інформаційних інфраструктур. Для досягнення поставленої мети необхідно визначити множину критеріїв, що характеризують поняття кіберстійкості. Це дасть можливість формулювати дефініції «кіберстійкість» для її подальшого використання при вирішенні поставлених задач сфери кібербезпеки та захисту інформації. В статті проведений аналіз поняття кіберстійкості, який засновується на підставі сформованої тридцятиоднокомпонентної множини критеріїв, дає можливість сформулювати дефініції, пов'язані з кіберстійкістю для її подальшого використання при вирішенні задач кібербезпеки та захисту інформації. На підставі сформованого в подальшому визначенні поняття кіберстійкості, можна, наприклад, розробити методи і моделі оцінювання її рівня.

***Ключові слова**: кібербезпека, кіберстійкість, критична інфраструктура, захист інформації, кібератака, кіберризики, кіберзагроза, кіберінциденти.*

ВСТУП

Україна вже давно є об'єктом регулярних і масштабних кібератак, які загрожують стабільному функціонуванню критичної інфраструктури. Європейський Союз також не є винятком. Особливу увагу приділяється координації та взаємодії в рамках міжнародних організацій для посилення кіберстійкості та забезпечення відповідальної поведінки держав у кіберпросторі. Форум кібердіалогу створив унікальні можливості для постійного спілкування, швидкого обміну кращими практиками для фахівців з України та ЄС, а також надав інформацію про кіберінциденти та кібератаки на критичну інфраструктуру, яка може мати спільних зовнішніх клієнтів.

Кіберстійкість дозволяє критично важливим елементам (наприклад, таким як, енергетика, дані, товари, тощо) продовжувати виконувати свої функції в надзвичайних ситуаціях. Так, Національна консультативна рада з питань інфраструктури визначила п'ять секторів, які слід включити до планування у забезпеченні кіберстійкості – це електроенергія, вода, транспорт, зв'язок і фінансові послуги. Кожен із цих секторів є важливим сам по собі, але при забезпеченні кіберстійкості слід враховувати їх взаємозалежність.

У зв'язку зі збільшенням кількості кібератак та інцидентів на об'єкти критичної інфраструктури перед спеціалістами постає проблема підвищення ефективності заходів безпеки, які забезпечать надійну та безперебійну роботу об'єктів критичної інфраструктури в цілому. Тому поняття кіберстійкість, управління кіберстійкістю, забезпечення кіберстійкості, оцінювання кіберстійкості набувають подальшої актуалізації [1]. Термін «стійкість» (пер. з англ. – resiliency) був дещо модифікований і на сьогодні використовується як кіберстійкість. Активно його почали обговорювати тільки декілька років тому, хоча в галузі безпеки він існує вже багато років. До поняття кіберстійкості, крім безпеки, відносять низку завдань і процесів, які стосуються інформаційних технологій (наприклад, резервування та відновлення після збоїв) і захисту бренду. Причому питання стійкості і безперервності сервісів в цьому понятті відносяться як до самої компанії, так і до зовнішніх підрядників, які надають такі послуги. Так, Держспецзв'язку визначили, що передумовою до появи кіберстійкості, як напрямку корпоративної кібербезпеки, стало прийняття компанія-ми факту про неминучість кібератаки. В поняття кіберстійкості також включають можливість підготуватися до атаки, забезпечення ефективної діяльності та протидії під час атаки, а також зниження можливих наслідків атаки на компанію. Важливим для підприємств є оцінювання стану кіберстійкості їх критичних інфраструктур для планування бюджету, що дозволяють забезпечити необхідний рівень кіберзахисту. Але для реалізації процесу оцінювання необхідно чітко розуміти що стоїть за зазначеним поняттям. Тому актуальною задачею є аналіз поняття кіберстійкості критичної інфраструктури.

Кіберстійкість стала національним пріоритетом у Сполучених Штатах на початку 2013 року після Президентської політичної директиви (PPD-21) щодо безпеки та стійкості критичної інфраструктури. Директива окреслює стратегію національних зусиль щодо посилення безпеки та стійкості основних об'єктів, таких як ядерні реактори, каналізаційні системи та греблі. Визначивши 16

критичних секторів інфраструктури, PPD-21 доручив Міністерству внутрішньої безпеки США (DHS) та іншим національним агентствам працювати разом, щоб оцінити та керувати кіберризиками в цих секторах. У цьому контексті важливими є питання забезпечення кіберстійкості інформаційної інфраструктури зазначених об'єктів, різноманіття понять якої описано в [1-35] і потребують певної систематизації.

Тому метою роботи є аналіз понять кіберстійкості для критичних інформаційних інфраструктур. Для досягнення поставленої мети необхідно визначити множину критеріїв, що характеризують поняття кіберстійкості. Це дасть можливість формулювати дефініції «кіберстійкість» для її подальшого використання при вирішенні поставлених задач сфери кібербезпеки та захисту інформації.

ОСНОВНА ЧАСТИНА

Так в [2] кіберстійкість – це здатність організації забезпечити розвиток діяльності (стійкість підприємства) за рахунок готовності до кіберзагроз, можливості реагування на них, засобів відновлення після кібератак. Кіберстійка організація здатна адаптуватися до відомих і невідомих криз, загроз, несприятливих факторів та викликів. У кінцевому підсумку кіберстійкість дозволяє підприємству процвітати за умов негативних чинників (кризи, пандемії, фінансової нестабільності тощо) і характеризується критеріями – відновлення після збоїв, стійкість.

Для забезпечення кіберстійкості пропонуються застосовувати комплексний аналітично керований підхід, в основі якого лежить тріада – Безпека, Ризики та Керівництво, що дозволить протистояти кібератакам, при цьому керуючись документом NCSI «Підвищення національної кіберстійкості» [3] і характеризується критеріями – керівництво NCSI, підготовка до атаки, протистояння.

Кіберстійкість банківської системи [4] визначається як властивість інформаційної інфраструктури банку забезпечувати функціонування його бізнес-процесів, продуктом яких є банківські та фінансові послуги, під час кібератак і кіберінцидентів, яка має постійно підтримуватися органами управління банку шляхом організації управління кіберризиками та впровадження заходів кіберзахисту. Відповідно, кіберстійкість платіжної системи визначається як спроможність платіжної організації, учасників платіжної системи, операторів послуг платіжної інфраструктури та розрахункового банку цієї платіжної системи запобігати, протистояти, стримувати та оперативно відновлюватися після кіберінцидентів та кібератак на неї. Тож в [4] кіберстійкість характеризується критеріями – безпека (захист), ризики, протистояння.

В джерелі [5] кіберстійкість визначається як спроможність національної системи протидіяти кіберзагрозам, зокрема кібертероризму, кібердиверсіям, кібератакам стосовно національної інформаційної інфраструктури. Для оцінювання рівня кіберстійкості країни розроблено ряд глобальних індексів: національний індекс кібербезпеки (National Cyber Security Index), глобальний індекс кібербезпеки (Global Cybersecurity Index) та національний індекс кіберпотужності (NCPI) і характеризується критеріями - національний індекс кіберезпеки (National Cyber Security Index), глобальний індекс кібербезпеки (Global Cybersecurity Index), національний індекс кіберпотужності (NCPI), управління кіберризиками, ідентифікація.

Так в [6] одним із ключових аспектів створення кіберстійкості є розуміння природи загроз, з якими стикаються організації. Кіберзлочинці стають все більш досвідченими, використовуючи передові методи проникнення в мережі, викрадення конфіденційних даних і зриву бізнес-операцій. Окрім зовнішніх загроз, є також потенціал внутрішніх загроз, оскільки співробітники, які мають доступ до конфіденційної інформації, можуть становити значні ризики, якщо їхні облікові записи скомпрометовано або якщо вони діють зловмисно. Важливим аспектом кіберстійкості є забезпечення того, щоб співробітники були досвідченими з питань кібербезпеки. Отже в [6] кіберстійкість характеризується такими критеріями – ризики, внутрішні і зовнішні загрози.

У [7] кіберстійкість визначається як інтегральний показник і характеризується кібернадійністю, яка відображає можливість виконувати свої завдання в складній системі управління критичною інфраструктурою в умовах інформаційних деструктивних впливів.

Європейський центральний банк поняття кіберстійкості формулює як спроможність захисту електронних даних і систем від кібератак, а також

відновлювати бізнес-операції у випадку успішної атаки [8] і характеризується такими критеріями, як відновлення після збоїв, безперервність сервісів, захист електронних даних.

У NIST SP 800-172 [9] кіберстійкість визначається як здатність передбачати, протистояти, відновлюватися та адаптуватися до несприятливих умов, стресів, атак чи компрометації систем, які використовують кіберресурси або підтримуються ними, що відповідає наступним критеріям: відновлення після збоїв, підготовка до атаки, зниження можливих наслідків атаки, управління та захист, запобігання. Таким чином відповідно до NIST SP 800-160 Vol. 2 Ред. 1 NIST SP 800-172A з NIST SP 800-160 Vol. 2 Ред. 1 кіберстійкість призначена для досягнення цілей, які залежать від кіберресурсів, у конкурентному кіберсередовищі.

Також у документі [10] кіберстійкість визначається, як здатність системи або інформаційної інфраструктури до оперативності реагування та адаптації до кіберзагроз, включаючи атаки, помилки, вразливості та відмови, збереження конфіденційності, цілісності та доступності інформації в умовах кібератаки, при виникненні кіберінцидентів або непередбачуваних змін та відповідає наступним критеріям: відновлення після збоїв, безперервність сервісів, зниження можливих наслідків атаки.

Кіберстійкість у [11] – це готовність до атак, системних збоїв, стихійних лих або людського фактору. Тож, кіберстійкість - це поєднання стратегій, процесів та технологій, які допоможуть підготуватися до будь-якого інциденту, пов'язаного з кіберпростором, та відреагувати на нього. Впровадивши належні заходи кібербезпеки та плани реагування на інциденти, організація стане більш стійкою та краще підготовленою до реагування на будь-які інциденти, які можуть виникнути. Загалом кажучи, згідно з NIST, кіберстійкість – це здатність підготуватися до «несприятливих умов», таких як кібератаки та інциденти, які загрожують конфіденційності, доступності або цілісності цифрових активів компанії, реагувати на них, відновлюватися та адаптуватися до них. Надійна стратегія кіберстійкості дозволяє організаціям продовжувати роботу навіть перед кіберштормами. Кіберстійка організація робить більше, ніж просто намагається запобігти кібератакам. Окрім надійного підходу до кібербезпеки, необхідно розробляти плани реагування та резервні плани, щоб забезпечити швидке відновлення та безперервність роботи навіть у разі виникнення інциденту чи атаки. Кіберстійкість є ключовим елементом сталого розвитку підприємства та стосується таких системних ресурсів, як персонал, процеси, безпека ланцюга поставок, практики управління ризиками.

Застосовуючи проактивний комплексний підхід до кібербезпеки [11], кіберстійкість мінімізує вплив кібератак на операції та репутацію, дозволяючи об’єктам продовжувати працювати ефективно та безпечно. Від GDPR і CCPA до HIPAA та GLBA, організації в усіх галузях повинні все частіше звертатися до регуляторів вимог під час розробки своїх стратегій кібербезпеки та реагування. Кіберстійкість є ключовим елементом дотримання правил і стандартів кібербезпеки та захисту. Впроваджуючи ефективні заходи кіберстійкості, організації відповідають вимогам і демонструють дотримання вимог захисту конфіденційної інформації та персональних даних. Кіберстійкість – це не лише технології, бо співробітники відіграють ключову роль у забезпеченні цілісності систем і організацій і, у разі порушення безпеки, вони забезпечують належну реакцію організації на інцидент. Забезпечення захисту конфіденційних даних і фізичних активів за допомогою вдосконалених внутрішніх процесів і операційної культури є важливим елементом стратегії кіберстійкості. Кіберстійкість вимагає передбачення нових атак за допомогою таких методів, як моделювання загроз і посилення захисту, перш ніж вони стануть уразливими. Cyber Resilience передбачає кіберінциденти та використовує проактивний підхід до планування та навчання для забезпечення безперервності бізнесу. Так, кіберстійкість у [11] характеризується наступними критеріями: відновлення після збоїв, керівництво NSCI «Підвищення національної кіберстійкості», підготовка до атаки.

Так, IT Governance [12], провідний світовий постачальник рішень для управління кіберризиками та конфіденційністю, приділяє особливу увагу кіберстійкості та пропонує розглядати кіберстійкість як здатність організації захищати, виявляти, реагувати на кібернетичні дії та відновлюватися після них. Завдяки стійкості, організації можуть пом’якшити вплив атаки та забезпечити

ефективну роботу. Відповідно, у [12], кіберстійкість характеризується такими критеріями, як відновлення після збоїв, адаптування до відомих і невідомих криз, управління та захист.

Згідно з дослідженням [13], кіберстійкість означає здатність організації виявляти, реагувати та швидко відновлюватися після інцидентів інформаційної безпеки. Підвищення кіберстійкості передбачає розробку плану, заснованого на оцінці ризиків, який передбачає, що система колись зазнає злому або атаки. Так у [13] характеристики кіберстійкості наступні: відновлення після збоїв, ризики, виявлення.

Тихоокеанська північно-західна національна лабораторія [14], провідний центр наукових відкриттів у галузі хімії, даних і геонаук, а також технологічних інновацій у сфері сталої енергетики та національної безпеки, зазначає, що кіберстійкість – це ширший підхід до кібербезпеки, спроба посилити захист системи проти потенційних атак. Незважаючи на те, що кібербезпека є ключовим елементом кіберстійкості, остання підтримує концепцію захисту системи, яка базується на припущенні, що системи повинні мати можливість продовжувати роботу та/або швидко відновлюватись у разі порушення віртуальних каналів [14]. Так в [14] характеристики кіберстійкості наступні: відновлення після збоїв, протистояння, виявлення.

Mimecast визначає кіберстійкість [15] як цілісний підхід до кібербезпеки, який охоплює широкий спектр стратегій, процесів, технологій і методів кібербезпеки, призначених для забезпечення безперервності діяльності організації, навіть у разі кібератаки чи кіберзагрози, що може порушити роботу організації, спричинивши простої, фінансові втрати, репутаційні збитки та можливі юридичні та регуляторні наслідки. Кіберстійкість відіграє ключову роль у разі виникнення кіберінциденту та гарантує, що організація може продовжувати виконувати свої критичні функції навіть під час або після інциденту, обмежуючи збої в роботі. Це означає, що кіберстійкість – це цілісний підхід до забезпечення кібербезпеки, який полягає у здатності подолати кібератаки та відновлюватися після них. Це запобіжний захід проти людських помилок, уразливості програмного забезпечення, апаратних проблем і неправильних налаштувань. У [15] характеристиками кіберстійкості є відновлення після збоїв, підготовка до атаки, протистояння.

У [16] Кіберстійкість означає здатність постійно виконувати задуманий результат, незважаючи на несприятливі кіберподії. Цю здатність можна розглядати на різних рівнях, як обговорюється в [16]. Кожен рівень пропонує свої унікальні методи та можливі засоби контролю кіберстійкості. Отже, здатність постійно досягати запланованого результату може стосуватися не тільки держави, а також і організації чи навіть конкретної IT-системи. Проте, щоб кіберстійкість була ефективною, її потрібно розглядати цілісно, на кількох рівнях і паралельно. Так в [16] основною характеристикою кіберстійкості є підготовка до атаки.

У [17] кіберстійкість – це здатність організації постійно досягати запланованих бізнес-результатів, незважаючи на несприятливі кіберподії. Вони можуть включати злам, інсайдерську загрозу, атаку програм-вимагачів або інші руйнівні впливи.

Якщо система є кіберстійкою, вона забезпечує конфіденційність, цілісність і доступність своїх даних, щоб протистояти кібератакам і відновлюватися після них.

Кіберстійкість, яка поєднує в собі кібербезпеку з принципами нульової довіри, безперервність бізнесу, відновлення кібербезпеки та стратегії організаційної стійкості, наразі є актуальною темою заходів з кібербезпеки, оскільки кількість і серйозність загроз продовжують зростати. Компанії змінюють свої підходи до кібербезпеки за допомогою рішень для захисту даних і керування даними, які є як проактивними, так і реактивними, щоб покращити кіберстійкість. Кіберстійкість важлива, оскільки всі підприємства, від комерційних підприємств до державних установ, освітніх установ і організацій охорони здоров'я в усьому світі, залежать від даних. Наприклад, 11 січня 2023 року тисячі рейсів у США були затримані через випадкове видалення файлів. Це хороший приклад того, чому кіберстійкість має вирішальне значення для операційної стабільності підприємств. Так, за оцінками, до 2031 року програми-вимагачі атакуватимуть кожні дві секунди, що коштуватиме організаціям 265 мільярдів доларів на рік. Тому, щоб операція була успішною, структуровані та неструктуровані дані організації повинні бути належним чином ідентифіковані, захищені та доступні лише

для уповноважених осіб. Кіберстійкість допомагає організаціям [17]:

• залишатися в робочому стані під час несприятливої події (наприклад, катастрофи, людської помилки, атаки програм-вимагачів або внутрішньої загрози);
• уникнути непотрібних простоїв;
• підтримувати безперервність діяльності;
• забезпечити безпеку даних;
• відповідати нормативним вимогам;
• захистити свою репутацію;
• уникати сплати викупу;
• виявляти та захищатись від зловмисників;
• швидко відновлюватись після інциденту.

Система кіберстійкості включатиме [17]: плани безпеки, включаючи резервне копіювання даних і можливості виявлення шкідливих програм; плани безперервності бізнесу, включаючи ціль відновлення та цільову точку відновлення; організаційні плани стійкості, такі як група реагування, менеджери зі зв'язків з громадськістю та виконавче спонсорство.

Найважливішим елементом будь-якої системи кіберстійкості є дотримання принципів безпеки Zero Trust. За замовчуванням «нульова довіра» – це принцип безпеки «ніколи не довіряй, завжди перевіряй». Організації, які дотримуються цього принципу, знають, що пристроям не слід регулярно або постійно довіряти, навіть якщо вони підключені до керованої корпоративної мережі, наприклад корпоративної локальної мережі, і навіть якщо вони були попередньо автентифіковані. Ефективна архітектура нульової довіри базується на трьох принципах: аутентифікація користувача/програми; аутентифікація пристрою; філософія довіри/недовіри.

Слабкою ланкою в стратегіях кібербезпеки багатьох організацій є спосіб організації захисту та керування їхніми неструктурованими даними [17]. Хоча кібербезпека має вирішальне значення, це лише один з елементів надійної стратегії кіберстійкості. Завдяки можливостям кібербезпеки організації можуть виявляти та захищатись від таких загроз, як програми-вимагачі або зловживання обліковими даними для доступу до конфіденційної інформації. Однак за допомогою надійної стратегії кіберстійкості організації можуть не тільки виявляти програми-вимагачі та інші загрози і захищатися від них, а й швидко реагувати та усувати без значного негативного впливу на організацію.

В організаціях важливими показниками кіберстійкості можуть бути [17]:

• частота виконання певних операцій, таких як регулярне резервне копіювання, сканування ІТ-систем на наявність уразливостей і загроз, а також встановлення оновлень антивірусного програмного забезпечення;
• надійність засобів контролю доступу, наприклад, за ролями, дозволами тощо;
• цільовий час відновлення (RTO), тобто час, потрібний системі для повернення до нормального стану;
• цільова точка відновлення (RPO), яка визначає, скільки даних організація може втратити до відновлення;
• кількість і типи інтеграції з провідними постачальниками рішень безпеки.

Таким чином в [17] за критерії кіберстійкості приймається: відновлення після збоїв, безперервність сервісів, підготовка до атаки, зниження можливих наслідків атаки, цільовий час (точка) відновлення.

У [18] кібербезпека має на меті мінімізувати можливість кібератаки та намагатися запобігти проникненню зловмисників. Стійкість передбачає вжиття заходів для ефективного виявлення, реагування та відновлення, якщо зловмиснику вдасться порушити захист кібербезпеки. Завдяки стійкості, транспортні зв'язки продовжуватимуть працювати безпечно, навіть, якщо зловмисник буде намагатися зламати системи керування повітряним, морським, автомобільним або залізничним транспортом. Тож у [18] критеріями кіберстійкості є відновлення після збоїв, ризики, підготовка до атаки, зниження можливих наслідків атаки, протистояння, управління та захист, виявлення.

Кіберстійкість у [19] відноситься до здатності організації продовжувати бізнес-операції, незважаючи на інциденти кібербезпеки або втрату даних. Щодня організації стикаються із завданням захисту своїх даних від внутрішніх і зовнішніх загроз. Кіберстійкість означає здатність компанії зменшувати збитки та швидко відновлювати критичні системи після зламу. Стійкість може протистояти як зовнішнім загрозам, таким як хакери та зловмисне програмне забезпечення, так і внутрішнім загро-

зам, таким як випадкове видалення. Оскільки програми-вимагачі є постійною загрозою, сьогодні жодна компанія не може бути повністю безпечною, покладаючись виключно на рішення кібербезпеки. Ось тут і вступає в дію стратегія кіберстійкості. В ідеальному двосторонньому підході рішення з кібербезпеки мінімізує ризик атак вторгнень, але коли вони неминуче відбуваються, для мінімізації впливу впроваджується надійна стратегія кіберстійкості, включаючи аварійне відновлення. Так у [19] критеріями кіберстійкості є наступні: надійність (кібернадійність), аутентифікація користувача\програми, філософія довіри\недовіри, кількість та типи інтеграцій з провідними постачальниками рішень безпеки.

Підвищення кіберстійкості є ключовим елементом робочої програми FSB (рада з фінансової стабільності) [20] щодо забезпечення фінансової стабільності. Кіберінциденти становлять загрозу стабільності світової фінансової системи. Серйозний кіберінцидент, якщо його не прийняти належним чином, може серйозно підірвати фінансову систему, включаючи критично важливу фінансову інфраструктуру, що призведе до ширших наслідків фінансової стабільності. Тому FSB здійснила низку дій щодо усунення кіберризиків. Таким чином, у [20] критеріями кіберстійкості є відновлення після збоїв, внутрішні, зовнішні загрози.

Для того, щоб організація стала стійкою до атак, необхідно змінити спосіб мислення, який змінить сприйняття ризиків та потенційних наслідків [21]. Організаціям необхідно розширити сферу участі вищого керівництва та почати концентруватися на бізнес-ризиках, а не лише на технологіях та засобах забезпечення безпеки. Це також передбачає здатність перерозподіляти пріоритети та переорієнтувати завдання та дії для пом'якшення наслідків збоїв. Стійкість організацій спрямована на покращення здатності передбачати, готуватися, реагувати та адаптуватися до інцидентів та криз, а також швидше відновлювати операції, тим самим обмежуючи та пом'якшуючи збитки для організації. Тож перелік процедур із забезпечення кіберстійкості, що наведені в [21], підвищують стійкість, змінюючи напрям процесу від зосередження уваги на захисних заходах до активного управління кіберінцидентами, реагування та відновлення після кіберкриз, а також швидшого відновлення операцій, тим самим обмежуючи збитки для організації. Такі процедури охоплюють стратегічні, технічні та експлуатаційні аспекти кіберстійкості. Так в [21] критерії кіберстійкості є наступні: відновлення після збоїв, підготовка до атаки, зниження можливих наслідків атаки.

В [22] кіберстійкість визначається як здатність до збереження та відновлення функціональності та життєздатності інформаційних систем і даних внаслідок кіберінцидентів, а також адаптивність до змін у внутрішніх та зовнішніх умовах і відповідає наступним критеріям: відновлення після збоїв, підготовка до атаки, зниження можливих наслідків атаки, виявлення.

ENISA [23] визначає кіберстійкість як можливість організацій та систем відновлюватися після кібератак та інших кіберінцидентів, а також пропонує застосовувати заходи для запобігання таким інцидентам і відповідає наступним критеріям: відновлення після збоїв, запобігання.

Схема визначення кіберстійкості від Cyber-ResilienceReview (CRR) [24] визначає кіберстійкість як здатність адаптуватись до негативних впливів і кіберзагроз, включаючи атаки, помилки та надзвичайні ситуації тощо, а також можливість системи відновлюватись після виникнення інциденту. Тобто в [24] за критерії кіберстійкості приймаються: відновлення після збоїв, адаптація до відомих і невідомих криз.

В [25] кіберстійкість – це здатність системи або мережі залишатися операційними та забезпечувати доступ до необхідних ресурсів в умовах кібервпливу, кібертероризму, кібершпигунства та інших кіберзагроз і відповідно кіберстійкість відповідає критеріям – надійність (кібернадійність) та кібервпливи.

У роботі [26-28] кіберстійкість визначається як здатність системи, бізнесу, організації передбачати, витримувати, відновлюватись і розвиватися в умовах деструктивних дій, кібератак на інформаційні ресурси, які являються критичними для функціонування. Тобто критеріями кіберстійкості є відновлення після збоїв, зниження можливих наслідків атаки, виявлення, запобігання, стримування, готовність до кіберзагроз.

В [29] кіберстійкість визначається як здатність протистояти зовнішнім загрозам, викликаними кіберризиками, відновлюватися та адаптуватися до

них. В [30] поняття кіберстійкості описується як здатність системи протистояти кібератакам, збоям і продовжувати працювати в погіршеному стані для виконання своєї місії. Таким чином, стійка до роботи CMS здатна протистояти збоям, спричиненим кібератаками, зберігаючи доступність, ефективність використання та коефіцієнт якості вище порогових значень погіршення до відновлення.

Також розроблені деякі програмні рішення дозволяють забезпечувати кіберстійкість. Так компанія [31], яка розробила ПЗ для підвищення кіберстійкості, визначає кіберстійкість як здатність готуватися до кібератак і витоків даних, реагувати на них і відновлюватися після них, продовжуючи при цьому ефективно працювати. Організація є кіберстійкою, якщо вона може захиститися від кіберзагроз, мати адекватне управління ризиками кібербезпеки та гарантувати безперервність бізнесу під час та після кіберінцидентів. Кіберстійкість, поряд з управлінням поверхневими атаками, з'явилася за останні кілька років, оскільки традиційних заходів безпеки, таких як тестування на проникнення та опитувальники безпеки, замало для мінімізації кіберризиків. Так в [31] виділяють чотири елементи кіберстійкості: управління та захист (сюди входить розвиток здатності виявляти, оцінювати та керувати кіберризиками, пов'язаними з мережами та інформаційними системами, у тому числі ризиками сторонніх та четвертих постачальників); виявлення та попередження (цей елемент передбачає використання безперервного моніторингу безпеки та управління поверхнями атак для виявлення аномалій та потенційних витоків даних до того, як буде завдано значної шкоди); реагування та відновлення (цей елемент передбачає впровадження адекватного планування реагування на інциденти для забезпечення безперервності бізнесу, навіть якщо система стала жертвою кібератаки); керування та забезпечення безпеки (останнім елементом є забезпечення того, щоб програма кіберстійкості контролювалася з боку керівництва організації).

Також існує чотири поширені загрози кіберстійкості, яким допоможе надійна стратегія кіберстійкості [31]:

1. Кіберзлочинність – злочини, вчинені проти окремих осіб або груп з метою навмисно завдати шкоди репутації жертви, завдати фізичної чи моральної шкоди або заподіяти жертві збитки прямо чи опосередковано з використанням Інтернету. Кіберзлочини зазвичай загрожують безпеці та фінансовому благополуччю людини, організації чи країни. Поширені кіберзлочини включають зараження шкідливим програмним забезпеченням, фішинг, цільовий фішинг, китобійні атаки та інші форми соціальної інженерії;

2. Хактивізм – використання комп'ютерних методів, таких як хакерство, як форма громадянської непокори для просування політичної програми чи соціальних змін. Поширені інциденти хактивізму в галузі кібербезпеки включають атаки типу «відмова в обслуговуванні» на критично важливу інфраструктуру та інформаційні системи, доксинг, відключення веб-сайтів, програми-вимагачі, здатні використовувати черв'яків, тайпсквоттінг, атаки «людина посередині» та витік інформації;

3. Кібершпигунство – це практика отримання секретів та інформації без дозволу або відома її власника. Кібершпигунство може бути формою промислового шпигунства або національною таємницею. Відсутність або погано налагоджений процес захисту інформації та відсутність навчання з питань кібербезпеки щодо того, яку інформацію можна і не можна публікувати в соціальних мережах, що і є частими причинами успішних атак кібершпигунства. Основні цілі кібершпигунства включають комерційну таємницю, інформацію про ланцюжок поставок, особисту інформацію, захищену медичну інформацію та ін.;

4. Управління безперервністю бізнесу – це процес створення систем запобігання та відновлення для боротьби з потенційними загрозами для компанії. Крім запобігання, мета полягає в тому, щоб забезпечити можливість виконання поточних операцій до та під час виконання аварійного відновлення.

Отже, в [31] критеріями кіберстійкості є відновлення після збоїв, безпека (захист), зниження можливих наслідків атаки, протистояння, кібервпливи.

В [32] кіберстійкість означає здатність підприємств знижувати ризик пошкодження своїх даних та операцій, а також відновлюватися неушкодженими після атаки. Замість покладатися на традиційний план аварійного відновлення, сучасним

організаціям необхідно перейти до кіберстійкого підходу, щоб забезпечити постійне обслуговування. Сьогоднішні організації розуміють, що питання в тому, коли, а не в тому, чи вони зіткнуться з кібератакою. Кіберстійкість – це здатність підготуватися до кібератаки, відреагувати на неї та відновитися після її виникнення. Кіберстійкість вирішує цю проблему, не обмежуючись профілактичними заходами, щоб постійно забезпечувати цілісність ваших критично важливих даних та знижувати ризики. Деякі організації використовують структури безпеки, наприклад, структуру кібербезпеки (CSF) Національного інституту стандартів та технологій (NIST), яка, для досягнення кіберстійкості, пропонує п'ять основних процедур: ідентифікація, захист, виявлення, реагування та відновлення. Цей тип стійкості вимагає рішення для відновлення, яке гарантує доступ до всіх даних без їх втрати у разі атаки, щоб робота системи могла бути відновлена та запущена без затримок. Відновлення даних є основою кіберстійкості. Для відновлення після кібератак потрібне сучасне рішення для управління даними та відновлення, яке забезпечує захист на декількох платформах, включаючи локальні, хмарні, багаторівневі сховища та програми SaaS. Ефективний план відновлення означає, що організація зможе уникнути простоїв, збоїв у роботі бізнесу та величезних фінансових втрат. Ефективний план відновлення означає, що організація зможе уникнути простоїв, збоїв у роботі та величезних фінансових втрат, коли зловмисники спробують скомпрометувати IT-середовище. Таким чином, стійкість IT, очевидно, є ключовим компонентом кіберстійкості. За допомогою застосунку Zerto організація може розробити комплексний план кіберстійкості, який допоможе впевнено протистояти постійно зростаючій кількості кіберзагроз. Завдяки вдосконаленому безперервному захисту даних та керуванню хмарними даними Zerto надає кілька варіантів відновлення, щоб мінімізувати час простою та втрату даних внаслідок кібератак, операційних втрат чи будь-якої катастрофи. І так в [32] критеріями кіберстійкості є відновлення після збоїв, зниження можливих наслідків атаки, протистояння, управління та захист.

В [33] досліджена модель зрілості потенціалу – перша у галузі хмара для забезпечення стійкості даних Druva. Сьогодні підприємствам потрібне рішення, яке автоматично масштабується вгору та вниз у будь-якому місці, забезпечуючи кіберстійкість даних у кількох хмарах по всьому світу. Революційне, хмарне та мультитенантне SaaS-рішення Druva використовує переваги простоти та масштабованості загальнодоступної хмари, надаючи єдине рішення для резервного копіювання та відновлення, аварійного відновлення, кіберстійкості, виявлення електронних даних та юридичного зберігання, забезпечення відповідності вимогам та криміналісти. Хмара Druva Data Resiliency Cloud забезпечує уніфікований і простий в управлінні захист даних для всіх робочих навантажень та кіберстійкість відповідає наступним критеріям – стійкість, безперервність сервісів, підготовка до атак.

TechTarget – американська компанія, яка пропонує маркетингові послуги на основі даних клієнтам технологій для бізнесу [34] зазначає, що кіберстійкість – це спроможність обчислювальної системи швидко відновлювати систему у випадку виникнення несприятливої ситуації. Кіберстійкість, хоч і не залежить від конкретної події, формується з часом і відноситься до підготовки, яку організація проводить для боротьби з загрозами та вразливістю, розроблених засобів захисту та ресурсів, які доступні для пом'якшення наслідків збою безпеки постфактум. Можливості кіберстійкості необхідні в IT-системах, критичній інфраструктурі, бізнес-процесах, організаціях та суспільствах. Кіберстійкість не слід розглядати як синонім відновлення, а скоріше як здатність підприємства обмежувати наслідки інцидентів безпеки та постійно забезпечувати бажаний результат, незважаючи на збій системи чи кібератаку. Концепція включає можливість відновлювати регулярні механізми захисту після таких подій, а також можливість постійно модифікувати ці механізми захисту для уникнення нових ризиків. Тож в [34] основними критеріями кіберстійкості є відновлення після збоїв, ризики, керівництво NSCI «Підвищення національної кіберстійкості», безперервність сервісів, управління та захист, виявлення. Було проведено дослідження постраждалих клієнтів, які не мали базових елементів керування безпекою та критично важливих елементів для підвищення кіберстійкості корпоративних систем. Результати ґрунтуються на взаємодії клієнтів із корпорацією Microsoft за минулий

рік [35] за показниками, які ґрунтуються на показниках вразливостей системи**:** незахищена конфігурація Active Directory; небезпечна конфігурація Azure Active Directory; застарілі протоколи автентифікації; застарілі алгоритми хешування; відсутність ізоляції привілеїв в Active Directory через модель рівня; невикористані робочі станції з привілейованим доступом; відсутність засобів керування привілеями доступу; зайві облікові дані адміністратора; прогалини в навичках операцій безпеки; прогалини в описі та інтеграції моніторингу безпеки; відсутність рішень SIEM\SOAR; неефективні процеси SOC та операційна модель; відсутність незмінних або придатних резервних копій; неефективні засоби запобігання втрат даних; відсутність виправлення та управління вразливістю; некеровані або застарілі програми; відсутність нульової довіри до впровадження систем безпеки; незахищений дизайн і конфігурація на хмарних платформах; відсутність практик SDL у DevOps. Таким чином в [35] основними критеріями кібербезпеки є безпека (захист), надійність (кібернадійність). Наведено наступні основні критерії огляду, які використовуються для визначення кіберстійкості (табл. 1): резервування – К1; відновлення після збоїв – К2; безпека (захист) – К3; ризики – К4; керівництво NSCI «Підвищення національної кіберстійкості» – К5; внутрішні, зовнішні загрози – К6; стійкість – К7; безперервність сервісів – К8; підготовка до атаки – К9; зниження можливих наслідків атаки – К10; адаптація до відомих і невідомих криз – К11; національний індекс кіберезпеки (National Cyber Security Index) – К12; глобальний індекс кібербезпеки (Global Cybersecurity Index) – К13; національний індекс кіберпотужності (NCPI)– К14; надійність (кібернадійність) – К15; захист електронних даних – К16; протистояння – К17; управління та захист – К18; виявлення – К19; аутентифікація користувача\програми – К20; філософія довіри\недовіри – К21; частота виконання певних операцій – К22; цільовий час (точка) відновлення (RTO) – К23; кількість та типи інтеграцій з провідними постачальниками рішень безпеки – К24; готовність до кіберзагроз – К25; управління кіберризиками – К26; запобігання – К27; стримування – К28; кібервпливи – К29; ідентифікація – К30; забезпечення конфіденційності, цілісності, доступності – К31.

Таблиця 1

Критерії визначення кіберстійкості

№ з/п	Номер джерела	Критерії (К)																													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1.	[1]	+	+	+				+	+	+	+	+				+										+						
2.	[2]		+					+																								
3.	[3]					+				+								+														
4.	[4]			+	+													+														
5.	[5]												+	+	+												+			+		
6.	[6]				+		+																									
7.	[7]															+																
8.	[8]		+						+								+															
9.	[9]		+							+	+							+										+				
10.	[10]		+						+		+																					
11.	[11]		+			+				+																						
12.	[12]		+									+								+										+	+	
13.	[13]		+		+															+												
14.	[14]		+															+		+												
15.	[15]		+							+								+														
16.	[16]									+																						
17.	[17]		+						+	+	+													+								
18.	[18]		+		+					+	+							+	+	+												

19.	[19]														+					+	+			+						
20.	[20]		+				+																		+					
21.	[21]		+					+		+	+																			
22.	[22]		+							+	+								+										+	
23.	[23]		+																							+				
24.	[24]		+																							+				
25.	[25]														+													+		
26.	[26]		+								+														+		+			
27.	[27]		+								+														+		+			
28.	[28]		+								+														+		+			
29.	[29]		+									+														+				
30.	[30]		+														+		+											+
31.	[31]		+	+							+						+											+		
32.	[32]		+								+						+	+												
33.	[33]							+	+	+																				
34.	[34]		+		+	+			+										+	+										
35.	[35]			+											+															

ВИСНОВКИ

Таким чином, проведено аналіз поняття кіберстійкості, який на підставі сформованої тридцятиоднокомпонентної множини критеріїв, які дають можливість сформулювати дефініцію «кіберстійкість» для її подальшого використання при вирішенні задач кібербезпеки та захисту інформації. Сформоване в подальшому визначення поняття кіберстійкості, може, наприклад, стати підставою розробки методів і моделей оцінювання рівня кіберстійкості.

ЛІТЕРАТУРА

[1] SPILNO [Electronic resource] spilno.org//Mode of access:// https: // spilno.org /article/kiberstiikist-scho-tse-yak-zabezpechyty-ta-yak-upravlyaty //(date of access: 20.12.2023).

[2] INTRACOM-UKRAINE [Electronic resource] intracom-ukraine.com//Mode of access:// https:// www.intracom-ukraine.com/cyber-security-cyber-resilience//(date of access: 20.12.2023).

[3] EGA [Electronic resource] ega.ee// Mode of access://https://ega.ee/uk/publication/ncsi-pidvish-hennya-natsionalnoyi-kiberstijkosti/∠(date of access: 20.12.2023).

[4] ПЛАТФОРМА ЛІГА:ЗАКОН [Electronic resource] ips.ligazakon.net//Mode of access: //https:// ips.ligazakon.net / document / TM065903 / (date of access: 20.12.2023).

[5] Онищенко С.В., Глушко А.Д., Маслій О.А. Кіберстійкість як основа національної безпеки України / Innovations and prospects of world science : Proceedings of XI International Scientific and Practical Conference, Vancouver, Canada, 22-24 June 2022. Vancouver: Perfect Publishing, 2022. С. 551-556.

[6] ts2 [Electronic resource] ts2.space // Mode of access://https://ts2.space/uk/%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D1%81%D1%82%D1%96%D0%B9%D0%BA%D1%96%D1%81%D1%82%D1%8C//(date of access: 20.12.2023).

[7] Мальцева І. Р., Черниш Ю. О., Овсянніков В. В. Аналіз методик оцінки кіберстійкості критичної інфраструктури. Кібербезпека: освіта, наука, техніка :електронне наукове видання. 2021. N 12. С. 29-35. Режим доступу: http://ek.kubg.edu.ua/cgi-bin/irbis64r_17/cgiirbis_64.exe?LNG=&Z21ID=&I21DBN=KUBG&P21DBN=KUBG&S21STN=1&S21REF=3&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21LOG=1&S21P03=K=&S21STR=%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D1%81%D1%82%D1%96%D0%B9%D0%BA%D1%96%D1%81%D1%82%D1%8C//(date of access: 20.12.2023).

[8] ECB [Electronic resource] ecb.europa.eu// Mode of access://https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html#:~:text=Cyber%20resilience%20refers%20to%20the,case%20of%20a%20successful%20attack//(date of access: 20.12.2023).

[9] NIST [Electronic resource] csrc.nist.gov//Mode of access: // https: // csrc.nist.gov / glossary/term/ cyber_resiliency//(date of access: 20.12.2023).

[10] Спеціальна публікація NIST 800-53B "NIST Cybersecurity Framework [Electronic resource] csrc.nist.gov // Mode of access: //https://csrc.nist.

gov/projects/cprt/catalog#/cprt/framework/version/ SP_800_53_5_1_1 /home// (date of access: 20. 12.2023).
[11] SPLUNK [Electronic resource] splunk.com // Mode of access:// https://www.splunk.com/en_us/blog/ learn/ cyber-resilience.html // (date of access: 20.12. 2023).
[12] itgovernance [Electronic resource] itgovernance. co.uk //Mode of access: // https: //www.itgovernance.co.uk/(date of access: 20.12.2023).
[13] CISCO [Electronic resource] www.cisco.com//Mode of access: // https: // www.cisco.com / c / en / us/ solutions/hybrid-work/what-is-cyber-resilience.html // (date of access: 20.12.2023).
[14] PNNL [Electronic resource] pnnl.gov//Mode of access://https: // www.pnnl.gov /explainer-articles/ cyber-resilience(date of access: 20.12.2023).
[15] MIMECAST [Electronic resource] mimecast.com// Mode of access://https://www.mimecast.com/content/cyber-resilience/(date of access: 20.12.2023).
[16] SPRINGER LINK [Electronic resource] link. springer.com// Mode of access: // https:// link. springer.com/chapter/10.1007/978-3-319-16486-1_31 //(date of access: 20.12.2023).
[17] Deborah, B., Graubart, R. (2011), "Cyber Resiliency Engineering Framework", MITRE Report, p. 37.
[18] COHESITY [Electronic resource] cohesity.com// Mode of access:// https://www.cohesity.com/glossary/cyber-resilience//(date of access: 20.12.2023).
[19] THALESGROUP [Electronic resource] thalesgroup.com // Mode of access:// https://www.thalesgroup.com/en/cyber-resilience//(date of access: 20. 12.2023).
[20] FSB [Electronic resource] fsb.org // Mode of access:// https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/cyber-resilience//(date of access: 20.12.2023).
[21] DELOITTE [Electronic resource] deloitte.com // Mode of access: // https://www.deloitte.com/ ru/ en/pages/risk/solutions/cyberresilience.html//(date of access: 20.12.2023).
[22] ISO/IEC 27032:2012 [Electronic resource] iso.org //Mode of access:// https://www.iso.org/ru/standard/76070.html (date of access: 20.12.2023).
[23] ENISA [Electronic resource] enisa.europa // Mode of access:// www.enisa.europa.eu (date of access: 20. 12.2023).
[24] CyberResilienceReview [Electronic resource] cisa.gov //Mode of access:// https://www.cisa.gov/resources-tools/services / cyber-resilience-review-crr (date of access: 20.12.2023).
[25] Шиповський В. Система показників оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури. Захист Інформації, Том 25, № 1, Січень-Березень 2023. С. 37-45.
[26] Juan F. Carías, SaioaArrizabalaga, LeireLabaka and JosuneHernantes. Cyber Resilience Progression Model. Applied Scitnces. 2020. Vol.10(21), 7393.
[27] R.S. Ross, R. Graubart, D. Bodeau, R. McQuaid, SystemsSecurityEngineering: CyberResiliencyConsiderationsfortheEngineeringofTrustworthySecureSystems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, 2019, Vol. 2. // Mode of access://https: //doi.org/10.6028/NIST.SP.800-160v2, (date of access: 20.12.2023).
[28] Brian West. Data Breach Preparation and Response. Breaches Are Certain, Impact Is Not. 2016, pp. 167-185. //Mode of access://https://doi.org/10.1016/ B978-0-12-803451-4.00007-1 (date of access: 20.12. 2023).
[29] Benoît Dupont, Clifford Shearinga, Marilyne Bernier, Rutger Leukfeldt. The tensions of cyber-resilience: From sensemaking to practice. Computers & Security Volume 132, September 2023, 103372//Mode of access: // https:// doi.org/10.1016/j.cose.2023.103372 //(date of access: 20.12.2023).
[30] Carlos Espinoza-Zelaya, Young Bai Moon. Framework for enhancing the operational resilience of cyber-manufacturing systems against cyber-attacks. Manufacturing Letters. Volume 35, Supplement, August 2023, pp 843-850. //Mode of access: //https: // doi.org / 10.1016/j.mfglet.2023.07.004// (date of access: 20.12.2023).
[31] UPGUARD [Electronic resource] upguard.com// Mode of access://https://www.upguard.com/blog/ cyber-resilience//(date of access: 20.12.2023).
[32] ZERTO [Electronic resource] zerto.com //Mode of access://https://www.zerto.com/resources/a-to-zerto/cyber-resilience (date of access: 20.12.2023).
[33] DRUVA [Electronic resource] druva.com //Mode of access:// https://www.druva.com/glossary/what-is-cyber-resilience//(date of access: 20.12.2023).
[34] TECHTARGET [Electronic resource] techtarget. com // Mode of access: // https: //www.techtarget. com/whatis / definition / cyber-resilience // (date of access: 20.12.2023).
[35] MICROSOFT [Electronic resource] microsoft.com // Mode of access://https://www.microsoft.com/ uk-ua /security / business/ microsoft-digital-defense-report-2022-cyber-resilience (date of access: 20.12. 2023).

ANALYSIS OF THE CONCEPT OF CYBER RESILIENCE OF CRITICAL INFRASTRUCTURE

Due to the increase in the number of cyber-attacks and incidents on critical infrastructure facilities, specialists face the problem of improving the effectiveness of security measures that will be able to ensure reliable and uninterrupted operation of critical infrastructure facilities as a whole. Therefore, the concepts of cyber resilience, cyber resilience management, cyber resilience provision, and cyber resilience assessment are gaining further relevance. The concept of cyber resilience, in addition to security, includes a number of tasks and processes related to information technology (e.g., backup and recovery after failures) and brand protection. Moreover, the issue of stability and continuity of services in this concept refers both to the company itself and to external contractors who provide such services. The prerequisite for the emergence of cyber resilience as a direction of corporate cyber security was the acceptance by companies of the fact that a cyber-attack is inevitable. The concept of cyber resilience also includes the ability to prepare for an attack, ensure effective operations and countermeasures during an attack, and reduce the possible consequences of an attack on a company. It is important for enterprises to assess the cyber resilience of their critical infrastructures to plan investments that enable them to provide the required level of cyber resilience. However, in order to implement the evaluation process, it is necessary to clearly understand what is behind this concept. Therefore, the analysis of the concept of cyber resilience of critical infrastructure is an urgent task. The purpose of the article is to analyse the concept of cyber resilience for critical information infrastructures. To achieve this goal, it is necessary to define a set of criteria characterizing the concept of cyber resilience. This will make it possible to formulate definitions of "cyber resilience" for its further use in solving the tasks of cyber security and information protection. The article analyses the concept of cyber resilience, which is based on the formed set of criteria consisting of 31 components. This makes it possible to formulate definitions related to cyber resilience for its further use in solving cybersecurity and information protection problems. Based on the subsequent definition of the concept of cyber resilience, it is possible, for example, to develop methods and models for assessing its level.

Keywords: cyber security, cyber resilience, critical infrastructure, information protection, cyberattack, cyberrisks, cyberthreat, cyberincidents.

Іванченко Євгенія Вікторівна, кандидат технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

Yevgenia Ivanchenko, candidate of technical sciences, professor, professor of the Department of Security of Information Technologies of the National Aviation University.
E-mail: evivancenko@gmail.com.
Orcid ID: 0000-0003-3017-5752.

Корченко Олександр Григорович, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, в.о. проректора з наукової роботи Національного авіаційного університету.

Oleksandr Korchenko, doctor of technical sciences, professor, laureate of the State Prize of Ukraine in the field of science and technology, acting vice-rector for scientific work of the National Aviation University.
E-mail: icaocentre@nau.edu.ua.
Orcid ID: 0000-0003-3376-0631.

Зарицький Олег Володимирович, доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

Oleg Zarytskyi, doctor of technical sciences, professor, professor of the Department of Security of Information Technologies of the National Aviation University.
E-mail: olegzaritskyi@gmail.com.
Orcid ID: 0000-0002-6116-4426.

Зибін Сергій Вікторович, доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

Serhii Zybin, doctor of technical sciences, professor, professor of the Department of Security of Information Technologies of the National Aviation University.
E-mail: zysv@ukr.net.
Orcid ID: 0000-0002-2670-2823.

Вишневська Наталія Сергіївна, старший викладач кафедри безпеки інформаційних технологій Національного авіаційного університету.

Nataliya Vishnevska, senior lecturer at the Information Technology Security Department of the National Aviation University.
E-mail: viserj@ukr.net.
Orcid ID: 0000-0001-9036-6556.