УДК 001.9
DOI: 10.31673/2409-7292.2022.040012

Костроміна М.О., Гарнатко Л.О.

КІБЕРСТІЙКІСТЬ І КІБЕРБЕЗПЕКА: У ЧОМУ РІЗНИЦЯ?

Розглянуто поняття кібербезпеки та кіберстійкості, а також проведено порівняльну характеристику даних понять. Ви дізнєтесь які заходи включає в себе кібербезпека та елементи проактивного плану дій для запобігання доступу зловмисників в корпоративну мережу. Розглянуто заходи, які повиннен включати в себе план кіберстійкості, щоб максимально мінімізувати негативний вплив кібератак. Досліджено механізми, які слід застосувувати як для кібербезпеки, так і для кіберстійкості.

Ключові слова: кібербезпека, стійкість, кіберстійкість, кібератака, відновлення.

Вступ

Кіберзлочини стрімко зростають як за складністю, так і за частотою. Щоб залишатися конкурентоспроможними в такому непередбачуваному середовищі, безпека даних, програм, мережі та критичних бізнес-процесів вашої організації має бути вашим головним пріоритетом. Традиційних рішень і методологій безпеки вже недостатньо для боротьби з сучасними складними кіберзлочинами. Бізнес повинен мати надійну стратегію кіберстійкості, яка дозволить підтримувати безперервність роботи до, під час і після інциденту кібербезпеки.

Аналіз досліджень

В публікації [1] визначено, що враховуючи швидку еволюцію загроз кіберсистемам, необхідні нові підходи до управління, які б стосувалися ризиків у всіх взаємозалежних сферах (тобто фізичних, інформаційних, когнітивних і соціальних) кіберсистем. Крім того, традиційний підхід захисту кіберсистем від виявлених загроз виявився неможливим. Тому подібно до того, як біологічні системи виробляють імунітет як спосіб реагування на інфекції та інші атаки, кіберсистеми також повинні адаптуватися до постійно мінливих загроз, які продовжують атакувати життєво важливі функції системи, і відновлюватися від наслідків напади. Автори пояснюють основні поняття стійкості в контексті систем, обговорюють відповідні властивості та обґрунтовують кіберстійкість. У статті також пропонується короткий опис способів оцінки кібервідмовостійкості системи та підходи до покращення кібервідмовостійкості.

У [2] зазначено, що зі зростанням занепокоєння щодо кіберстійкості зростає й інтерес до показників, які можна використовувати для порівняння альтернатив або оцінки прогресу щодо їх покращення. У статті представлені спостереження щодо показників кіберстійкості, взяті з досвіду, семінарів і літератури, які можуть бути використані для оцінювання кіберстійкості особистості, корпорації або держави.

У [3] показано, що технологічний прогрес і нові методи та процедури кібербезпеки є опорою для «соціального блага», з одного боку. З іншого боку, вони розширили ландшафт для збільшення кількості кіберінцидентів і витоку даних. Це усвідомлення того, що кіберінцидентів неможливо повністю уникнути, зробило кіберстійкість надзвичайно важливою передумовою будь-якої комплексної та надійної стратегії кібербезпеки. Незважаючи на важливість, існує дуже мало досліджень щодо кібервідновлення, як основного аспекту кіберстійкості та стандарту кібербезпеки. У статті автори розробили комплексну операційну структуру кібервідновлення. Крім того, автори показують, як реалізується скорочена версія структури, з урахуванням того факту, що не всі організації мають однаковий розмір.

Мета цього дослідження: обґрунтувати заходи побудови кіберстійкості організації

Завдання дослідження: дослідити теоретичні аспекти шляхів побудови кіберстійкості.

Однієї успішної кібератаки достатньо, щоб спричинити хаос, завдати величезних фінансових втрат або, у крайньому випадку, назавжди закрити бізнес. Тому кіберстійкість важлива для виявлення, оцінки, управління, пом’якшення та відновлення після зловмисних атак. Продумана стратегія кібервідмовостійкості не тільки допомагає захистити критично

важливі системи, програми та дані, але й забезпечує швидке відновлення та безперервність бізнесу в умовах руйнівних кіберінцидентів. Комплексна програма кібервідмовостійкості допоможе бізнесу підтримувати стабільну діяльність і залишатися на плаву навіть під час кризи.

Для того щоб краще розібратись в понятті "кіберстійкість" та принципах її побудови, пропоную почати з основ, а саме з розуміння що таке стійкість та бізнес стійкість.

Стійкість – це властивість за значенням стійкий. В академічному тлумачному словнику ми можемо побачити наступні пояснення слова "стійкий":

1. Здатний твердо стояти, триматися, не падаючи, не коливаючись.
2. Який довго зберігає і виявляє свої властивості, не піддається руйнуванню і т. ін.
3. Для якого характерні стабільність, постійність, сталість.
4. Здатний витримати зовнішній вплив, протидіяти чомусь.

Тобто стійкість – це здатність протидіяти негативним факторам та зберігати і виявляти свої властивості, не піддаватися псуванню, руйнуванню, незважаючи на зовнішні впливи.

Якщо розглядати стійкість у розрізі бізнесу, то це здатність організації швидко адаптуватися до збоїв, зберігаючи при цьому безперервні бізнес-операції та захищаючи людей, активи та загальний капітал бренду. Стійкість бізнесу виходить за рамки аварійного відновлення і безперервності бізнесу, пропонуючи стратегії після катастрофи, щоб уникнути дорогих простоїв, посилити вразливі місця та підтримувати бізнес-операції в умовах додаткових неочікуваних негативних зовнішніх впливів [4].

Стійкість бізнесу починається з розуміння того, що бізнес-процеси та робочі процеси мають бути збережені, щоб організації вижили в разі несподіваних подій. Серед важливих проблем планування стійкості бізнесу є людський фактор. Люди повинні бути підготовлені та навчені тому, як реагувати на хаотичну ситуацію.

План стійкості бізнесу іноді називають планом безперервності бізнесу (BCP). Стійкість є результатом різних підходів до готовності, включаючи безперервність бізнесу, аварійне відновлення технологій, управління кризами, управління ризиками та управління інцидентами [4].

Стійкість бізнесу включає різні елементи загальної стійкості, такі як організаційна стійкість, операційна стійкість, кіберстійкість і стійкість ланцюга поставок. Розширення терміну відображає те, наскільки важливою стала стійкість для підприємств, урядів та інших організацій.

Чому планування стійкості бізнесу є важливим?

Тепер уже недостатньо просто відновити бізнес-операції та критично важливі програми після стихійного лиха, кібератаки чи іншої події. Організації повинні бути готові адаптуватися до змін обставин. Як показала криза COVID-19, компаніям довелося швидко пристосовуватися до мінливого робочого середовища, яке включало підтримку віддаленої роботи та гібридних установок [4].

В 2022 році Україна зіткнулася ще з однією кризою – війна. Це призвело до масових кібератак не тільки на інфраструктуру країни, а також на великий та середній бізнес. Повітряні тривоги, обстріли, планові та аварійні відключення електроенергії – такі реалії реалії сьогодення. Бізнесу, щоб вижити, необхідно вміти швидко пристосовуватись до змін, наприклад, орендувати підвальні приміщення чи офіси з бомбосховищем, які облаштовані альтернативним джерелом електроенергії, щоб можна було працювати незважаючи на відключення електроенергії та забезпечити безпеку співробітникам під час повітряних тривог. А також важливо пам'ятати не тільки про безпеку співробітників, але і про безпеку активів, якими володіє організація.

Організації зобов'язані продовжувати свою діяльність, якщо тільки обставини, як-от злиття, не унеможливлюють це. Акціонери та інші зацікавлені сторони очікують, що бізнес продовжуватиме працювати, незважаючи на ймовірність руйнівної події, яка зашкодить фірмі.

У багатьох випадках повернення до колишніх норм може бути недостатнім; старі методи можуть не відповідати тому, як зараз працює бізнес. Стійкість виходить за рамки суворої безперервності бізнесу та DR, забезпечуючи гнучкість, адаптивність і стійкість, необхідні організаціям для адаптації до довгострокових змін у своїй роботі [4].

Що таке кібербезпека?

Кібербезпека полягає в захисті від кібератак, які націлені на корпоративні мережі компанії. Щодо кіберстійкості, то експерти визначають її як реакцію компанії після кібератаки та те, як вона відновиться. На цьому етапі кібербезпека та кіберстійкість представлені як дві окремі операції

Кібербезпеку можна оцінити як першу фазу кіберстійкості в тому сенсі, що будь-яка компанія повинна інтегрувати у свою стратегію кіберстійкості етап кібербезпеки [5].

Концепція кібербезпеки базується на ряді різних процесів, пристроїв, технологій, людських операцій і режимів управління, які впроваджуються для забезпечення захисту комп'ютерних мереж, цифрових активів, а також цифрових систем компанії.

Таким чином, заходи кібербезпеки впроваджуються для запобігання доступу хакерів до мережі та комп'ютерних систем компанії. Ці заходи є частиною так званого проактивного плану дій, який може включати такі елементи [5]:

- Впровадженний процес своєчасного оновлення всього програмного забезпечення та операційних систем.
- Встановлення та коректне налаштування антивірусу та десктопних фаєрволів.
- Дотримання всіх стандартів відповідності для забезпечення захисту конфіденційних даних користувачів.
- Забезпечення безпеки служб і пристроїв від численних зловмисних дій, таких як крадіжка або віруси.
- Блокування всіх екранів комп'ютера.
- Підвищення обізнаності та навчання працівників щодо обов'язку забезпечувати безпеку виконання їхніх щоденних завдань.
- Забезпечення фізичної безпеки приміщень компанії.

Завдяки всьому цьому пакету кібербезпеки організації матимуть більш стабільне становище, яке дозволить їй діяти як бар'єр проти зловмисників і запобігати їх спробам проникнути в їх комп'ютерні системи.

Що таке кіберстійкість?

Поняття кіберстійкість не є настільки поширеним та популярним, як кібербезпека. Більш детельно почали вивчати дане питання відносно нещодавно, хоча поняття існує вже багато років.

Кіберстійкість, окрім безпеки, включає в себе ряд процесів та завдань, які відносяться до захисту бренду і інформаційних технологій, наприклад, резервування та відновлення після збоїв та ін. [6].

Передумовою до появи кіберстійкості як напрямку корпоративної кібербезпеки стало прийняття компаніями факту про неминучість кібератаки. Кіберустійкість дозволяє підготуватися до атаки, забезпечує ефективну діяльність і протидію під час атаки, а також знижує можливі наслідки атаки на компанію (рис.1) [6].

Зіткнувшись із поширенням кібератак, не всі заходи безпеки є абсолютно безпомилковими. Саме тут кіберстійкість відіграє ключову роль завдяки впровадженню вдосконалених превентивних заходів, щоб максимально мінімізувати негативний вплив кібератак. До них, зокрема, відносяться [5]**:**

- Розроблено та впроваджено план щодо резервного копіювання в автономному режимі.
- Навчання персоналу щодо питать кібергігієни та поводження з корпоративними даними.
- Розгляд планів відновлення після проблем зі зв'язками з громадськістю, спричинених впливом кібератаки третьої сторони.

- Виконання на регулярній основі вправ із симуляції атак для підвищення готовності бізнесу у разі кібератаки.
- Створенно план безперервності бізнесу.

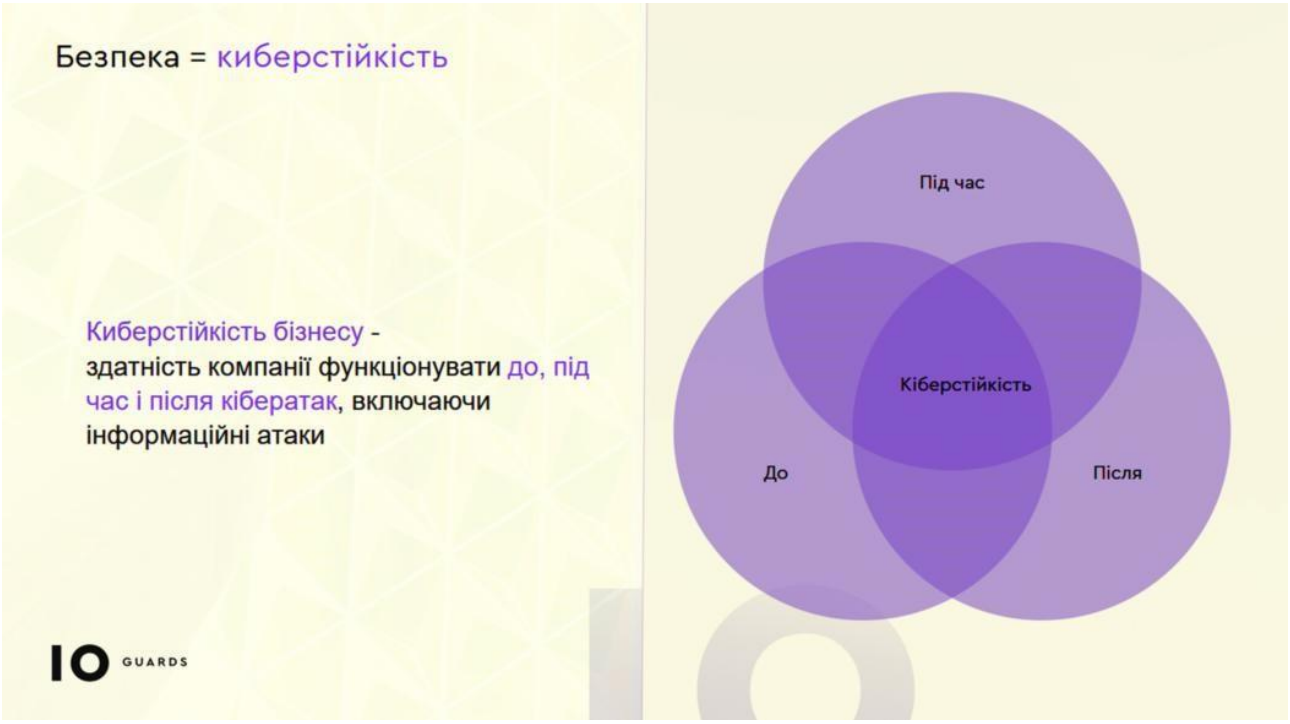

Рис. 1. Кіберстійкість бізнесу [6]

Кіберстійкість є важливою та незамінною концепцією для будь-якої організації, оскільки вона дозволяє їй забезпечити оптимальний захист від можливих вразливостей у майбутньому, а також максимально обмежити шкоду та втрати, спричинені кібератаками. До цього додається можливість створення вичерпного звіту про фазу після атаки, що дозволяє краще зрозуміти наслідки кібератаки.

Яка різниця між кібербезпекою та кіберстійкістю?

У той час як кібербезпека зосереджується на проактивних діях з метою надання допомоги та підтримки компанії в її боротьбі зі зростаючим поширенням кібератак, таких як програми-вимагачі та шкідливе програмне забезпечення та програми, кіберстійкість, зі свого боку, стосується потенціалу, який може мати компанія щоб максимально обмежити збитки, відновивши роботу у звичному режимі після кібератаки. Крім того, те, що відрізняє кібербезпеку від кіберстійкості, полягає в тому, що перша зосереджена на обмеженні загроз ззовні, тоді як кіберстійкість втручається у зовнішні загрози, такі як програми-вимагачі, а також *у* внутрішні загрози, які виникають у формі людської помилки [6].

Які механізми слід прийняти для застосування як для кібербезпеки, так і для кіберстійкості?

Щоб мати можливість легко інтегрувати дві концепції одночасно, а саме кібербезпеку та кіберстійкість, можна застосувати наступні практики [5]:

Виконання симуляційних тестів: ця практика актуальна в рамках запобігання та, перш за все, підготовки до боротьби з можливою реальною кібератакою. Це дозволяє компанії передбачити дії, які необхідно вжити у випадку атаки, шляхом моделювання інцидентів безпеки, а також дає змогу покращити стратегію кібербезпеки та кіберстійкості компанії.

- **Виконання регулярних резервних копій даних та систем:** після кібератаки компанія обов'язково має відновити свою нормальну діяльність і за короткий час відновити роботу у звичайному режимі. Для того, щоб досягти цього, дуже важливо, щоб він створював

резервні копії своїх даних на регулярній та постійній основі. Звичайно, щоб ці резервні копії були надійними, важливо робити їх в окремій мережі, щоб захистити їх від рук зловмисників. Якби дані були вкрадені або втрачені, компанії було б набагато простіше відновити їх і, отже, ефективніше та швидше забезпечити кіберстійкість.

Регулярне навчання кібербезпеці та кіберстійкості під час обговорення з радою директорів: належна підготовка всього персоналу в компанії на випадок кібератаки є вирішальним кроком, який необхідно зробити. Співробітники повинні стежити за всіма засобами, що дозволяють захистити дані компанії від потенційних кібератак. Важливо знати, що це стосується всього персоналу, включно з радою директорів, яка найчастіше знаходиться в певному розриві з технічно-технологічними аспектами. Необхідно переконатися, що всі співробітники глибоко розуміють заходи безпеки та знають, як їх застосовувати у разі кібератаки. Обидві концепції, будь то кібербезпека чи кіберстійкість, переслідують одну мету, а саме: захист даних компанії від можливих зловмисних кібератак.

Висновки

Кіберстійкість – це концепція, яка об'єднує безперервність бізнесу, безпеку інформаційних систем і стійкість організації. Тобто концепція описує здатність продовжувати досягати запланованих результатів, незважаючи на складні кіберподії, такі як кібератаки, стихійні лиха або економічні спади. Іншими словами, виміряний рівень кваліфікації та стійкості до інформаційної безпеки впливає на те, наскільки добре організація може продовжувати бізнес-операції в умовах дестабілізаційних впливів у кіберпросторі.

Стратегія кіберстійкості життєво важлива для безперервності бізнесу. Це може надати переваги, крім підвищення рівня безпеки підприємства та зниження ризику впливу на його критичну інфраструктуру. Кіберстійкість також допомагає зменшити фінансові втрати та репутаційну шкоду. І якщо організація отримує сертифікат кіберстійкості, вона може викликати довіру у своїх клієнтів і клієнтів. Крім того, кіберстійка компанія може оптимізувати цінність, яку вона створює для своїх клієнтів, збільшуючи свою конкурентну перевагу завдяки ефективній та ефективній діяльності.

Перелік посилань

1. Kott, Alexander. (2018). Fundamental Concepts of Cyber Resilience: Introduction and Overview.
2. Bodeau, Deborah J. and Richard D. Graubart. "Cyber Resilience Metrics: Key Observations." (2016).
3. C. Onwubiko, "Focusing on the Recovery Aspects of Cyber Resilience," 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2020, pp. 1-13.
4. What is business resilience? Paul Kirvan May 2022 https://www.techtarget.com/searchcio/definition/business-resilience
5. Cyber Resilience and Cybersecurity: what is the difference? URL: https://www.eurotechconseil.com/en/blog/difference-between-cyber-security-and-cyber-resilience/#:~:text=Experts%20on%20the%20subject%20will,and%20how%20it%20will%20recover.
6. Кіберстійкість – що це, як забезпечити та як управляти, 10 Guards, 2018. URL: https://spilno.org/article/kiberstiikist-scho-tse-yak-zabezpechyty-ta-yak-upravlyaty

Надійшла: 02.12.2022 Рецензент: д.е.н., професор Легомінова С.В.