ЩОДО ВИЗНАЧЕННЯ ТЕРМІНУ «КІБЕРБЕЗПЕКА»

НТУ «Дніпровська політехніка»

Павлов С.О.
Науковий керівник: ст.викл. Войцех С. І.

Одним із найважливіших питань 21 сторіччя для людства є забезпечення продуктивної роботи у різних сферах життєдіяльності і відповідне забезпечення безпеки у цих сферах. Міжнародною тенденцію з початку цифрової революції кінця 20 століття і донині стає посилення впливу інформаційної складової на всі сфери життя: від повсякденного життя звичайних громадян, процесів в бізнесі і до функціонування держав. З розвитком інформаційних систем ще більш актуальним постає питання забезпечення безпеки взаємозв'язку між такими системами і користувачами.

Першою базовою системою, що змогла зібрати і описати взаємодію інформаційних систем і необхідність її захисту, стала інформаційна безпека – процес збереження властивостей інформації. Проте з плином часу до простору інформаційної безпеки додається поняття «кібернетична безпека» або «Cyber Security». Вважається, що цей термін виник всередині цих систем приблизно в середині 1990-х років, коли в уряді США стали досліджувати цю тему [1].

На відміну від визначення «інформаційна безпека», з визначенням «кібернетична безпека» виникають питання і розходження на рівні спеціалістів в поглядах, що представлені у наукових статтях, міжнародних стандартах, а також на законодавчому рівні країн. Неоднозначність визначення терміну «кібербезпека» створює необмежену кількість сфер, в яких його будуть використовувати. Це у свою чергу призводить до відсутності обмежень щодо сфери кібернетичної безпеки.

Тому представляє інтерес порівняльний аналіз поглядів на визначення терміну «кібербезпека» в наукових публікаціях, в законодавчих документах на рівні держав, в міжнародних стандартах і однозначної дефініції цього терміну.

Так, проблемні аспекти дефініції та розмежування областей використання терміну «кібербезпека» викладено у науковій статті «Визначення Кібербезпеки» Дена Крайгена, Надії Діакун-Тхібаулт і Ренді Пурс[2] зведені до такого визначення: «Кібербезпека – це організація і збір ресурсів, процесів і структур, які використовуються для захисту кіберпростору і систем, що використовуються у ньому, від подій, що порушують(де юре) права власності(де факто)».

З цього визначення витікає, що кібербезпека – це процес захисту кіберпростору і систем в ньому від невизначених загроз. Але такому визначенню не вистачає конкретизації визначення «кіберпростору» та розширення дефініції подій, що порушують не лише права власності, а і інші складові того, що необхідно захищати. Інциденти безпеки можуть відбуватися без порушень прав власності, а і через внутрішні загрози.

Інше визначення було розглянуто в науковій публікації Баранова О.А. «Про тлумачення та визначення поняття "кібербезпека"»[3], а саме:

«…кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації».

На відміну від визначення Дена Крайгена та ін., визначення Баранова О.А. розуміється як стан захищеності.

Аналіз семантичної подібності щодо використання пов’язаних слів у визначеннях стосовно інформаційної безпеки і кібербезпеки наведено у статті «На шляху до більш характерного визначення кібербезпеки» журналу цифрової криміналістики, безпеки та права[4]. Однією з основних особливостей цієї статті є те, що в ній проаналізовано цілий ряд різноманітних джерел з широким трактуванням визначень методів захисту в кіберпросторі.

В Законі України «Про основні засади забезпечення кібербезпеки України»[5] кібербезпеку визначено як «забезпечення життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору».

Отже, можна зробити висновок, що одним із головних призначень кібербезпеки є не тільки забезпечення нормального функціонування технічних і комунікаційних систем, а і забезпечення нормального функціонування заснованих на них соціально-технічних систем.

В законах США «Акт про поширення інформації про кібербезпеку»[6] і «Акт про Кібербезпеку»[7] відсутнє пряме визначення кібербезпеки, проте дано чітке визначення термінів «загрози кібербезпеці» і «індикатори кібер загроз». Таким чином термін кібербезпека детально розкривається через засоби захисту від цих загроз.

У міжнародному стандарті ISO 27000 «Інформаційні технології – Методи захисту – Системи управління інформаційної безпекою інформації – Огляд і словник»[8] визначено поняття «інформаційна безпека» (information security) – «збереження конфіденційності, цілісності і доступності інформації, та інших її властивостей, таких як: автентичність, відстежуваність, неспростовність та надійність». Через це можна зробити висновок, що кібербезпека – це розширення поняття інформаційна безпека, тому що окрім захисту інформації і систем, необхідно захищати соціальну і соціально-технічну складову інформації. Із цього можна зробити висновок, що соціальна складова кіберзахисту охоплює будь-які суміжні сфери, в яких необхідно захищати інтереси особистості, окремої групи людей, суспільства або держави.

В публікації Агентства Європейського Союзу з питань мережевої та інформаційної безпеки [9] розглянуто такі домени кібербезпеки, як:

1. Комунікаційна безпека.
2. Операційна безпека.
3. Інформаційна безпека.

4. Фізична безпека.
5. Публічна/Національна безпека.

Слід зазначити, що розглядаючи міжнародні стандарти сфери інформаційних технологій із забезпечення інформаційної безпеки ISO/IEC 27 серії, важливою складовою інформаційної безпеки і кібербезпеки є ризик-орієнтований підхід, що уніфікує і значно спрощує методологію аналізу, вимірювання і подальшого усунення небажаних подій.

На основі результатів проведеного аналізу аспектів визначення термінів «кібербезпека» і «інформаційна безпека», можна зробити наступне припущення – загальний термін «кібербезпека» охоплює усі види людської діяльності, що використовуються у інформаційних системах та можуть мати комунікаційні мережі, а тому не може включати в себе особливості і винятки такої діяльності.

Таким чином, вважаємо за доцільне виділити такі основні домени, в яких визначена необхідність забезпечення захищеності життєво важливих інтересів особистості, окремої групи людей, суспільства або держави, і надати визначення окремим термінам цих доменів, які будуть містити в собі основну методологію щодо мінімізації настання небажаних подій.

Це можуть бути такі домени, що потребують подальшого перегляду і доопрацювання, як:

1. Національна кібербезпека
2. Кібербезпека критичної інфраструктури
3. Кібербезпека джерел інформації
4. Комунікаційна кібербезпека
5. Кібербезпека робочого процесу

Перелік посилань:

1. Stubley D. What is Cyber Security? – Режим доступу : https://www.7elements.co.uk/resources/blog/what-is-cyber-security/

2. “Defining Cybersecurity” Dan Craigen, Nadia Diakun-Thibault, and Randy Purse https://www.researchgate.net/publication/267631801_Defining_Cybersecurity

3. Баранов О.А., ПРО ТЛУМАЧЕННЯ ТА ВИЗНАЧЕННЯ ПОНЯТТЯ “КІБЕРБЕЗПЕКА” – Режим доступу : http://ippi.org.ua/sites/default/files/14boavpk.pdf

4. Daniel S., Rabih B., Julie W. Towards a More Representative Definition of Cyber Security – Режим доступу : https://commons.erau.edu/cgi/viewcontent.cgi?article=1476&context=jdfsl#:~:text=%E2%80%9CCybersecurity%20is%20the%20collection%20of,environment%20and%20organization%20and%20assets.%E2%80%9D

5. Про основні засади забезпечення кібербезпеки України: Закон України від 15.12.2021 № 2163-VIII// Відомості Верховної Ради (ВВР), 2017, № 45, ст.403 – Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19

6. Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015 – Режим доступу :

https://www.cisa.gov/sites/default/files/publications/CISA_PCL_Guidelines_Periodic_Review_2020_final.pdf

7. Cybersecurity Act Of 2015 – Режим доступу : https://www.intelligence.senate.gov/sites/default/files/legislation/Cybersecurity-Act-Of-2015.pdf

8. ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary – Режим доступу : https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

9. Definition of Cybersecurity Gaps and overlaps in standardisation V1.0 DECEMBER 2015. – European Union Agency For Network And Information Security – Режим доступу : https://www.enisa.europa.eu/publications/definition-of-cybersecurity