УДК 351.865(477)

ЗАГОСТЕННЯ ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

INCREASING PROBLEMS OF CYBERSECURITY PROTECTION

Л.О. Українська*[1] *, д.е.н. професор, Н.І.Шифріна*[2]*, к.е.н., доцент *Харківський Національний економічний університет імені Семена Кузнеця (м. Харків)*

Ukrainska L O. ***Doctor of Sciences in Economics, professor*** [1] ***,***
Shyfrina N. I.[2] ***PhD (Economics), Associate professor***
Simon Kuznets Kharkiv National University of Economics (Kharkiv)

У сучасному світі, де технології проникають у всі аспекти життя, кібербезпека стала найважливішим компонентом як національної, і глобальної безпеки. Ландшафт кіберзагроз стає все більш складним, регулярно з'являються нові типи атак, такі як програми-вимагачі, фішинг, DDoS та атаки на критичну інфраструктуру. Кіберзлочинці активно використовують штучний інтелект та машинне навчання для підвищення ефективності своїх методів. Масштаби кібератак постійно зростають, зокрема щодо державних органів, корпорацій, фінансових установ, приватних осіб [1]. Критична інфраструктура, включаючи енергетичні системи, транспортні мережі та комунікаційні системи, стає особливо вразливою, що несе серйозні ризики для суспільної безпеки та економічної стабільності.

Однією з актуальних проблем у цій галузі є гостра нестача кваліфікованих фахівців з кібербезпеки, що обмежує здатність держав та організацій ефективно протидіяти кіберзагрозам. Крім того, законодавчі рамки в багатьох країнах відстають від цифрового середовища, що швидко розвивається, вимагаючи термінової модернізації правового простору. Проте, незважаючи на ці труднощі, активізуються міжнародне співробітництво, обмін інформацією, технологіями та передовим досвідом, створюються глобальні центри реагування на кіберзагрози. Технологічні досягнення також відкривають нові можливості для захисту, при цьому штучний інтелект, машинне навчання та блокчейн використовуються для зміцнення систем кібербезпеки. Крім того, підвищення поінформованості громадськості про кіберризики та стратегії запобігання грає важливу роль у побудові стійкого цифрового суспільства [2].

Загалом кібербезпека є однією з найважливіших проблем сучасного світу. Для забезпечення безпеки в цифровому просторі необхідні скоординовані зусилля урядів, корпорацій та громадян. DDoS-атака (розподілена відмова в обслуговуванні) – це тип атаки, що спрямована на відмову у обслуговуванні. Внаслідок такої атаки цільовий мережевий ресурс отримує безліч запитів, які він може обробити. Джерелом цих

шкідливих запитів часто є ботнети, які складаються в основному з комп'ютерів, що належать звичайним користувачам, які були заражені шкідливим програмним забезпеченням. Великі DDoS-атаки націлені на урядові та організаційні веб-сайти, а також провідні IT-корпорації, такі як Amazon, Yahoo, Microsoft і т.інш.

Поряд із цими атаками також збільшилася кількість атак на дрібніші, «середні» веб-сайти, які раніше не вважалися привабливими цілями для кіберзлочинців. Однак, зі зростанням їх важливості, перерви в їх роботі можуть бути критичними.

У той самий час мотиви дій кіберзлочинців змінилися. Якщо раніше DDoS-атаки часто були викликані протестами чи хуліганством, то сьогодні DDoS-атаки все частіше використовуються для шантажу та здирництва. Це переміщає DDoS-атаки зі сфери індивідуальних протестів у сферу злочинного підприємництва, яке тепер виходить за рамки простого вимагання та також використовується екстремістськими та терористичними організаціями. У всьому світі атаки на урядові веб-сайти стали звичайним явищем, особливо перед виборами чи важливими політичними подіями.

Якщо порушити роботу великого ресурсу за допомогою активних контрзаходів складно, то щоб паралізувати менший ресурс буде достатньо менш потужної атаки з меншим ботнетом. Обслуговування та експлуатація таких ботнетів обходяться дешевше, і їх може створити більша кількість кіберзлочинців [3]. Фактична відсутність адекватних контрзаходів робить загрози безпеці, репрезентовані регіональними ресурсами DDoS-атак, особливо значними. З одного боку, більші заходи протидії можуть бути ефективно використані проти таких атак. З іншого, - впровадження та підтримання таких заходів економічно витратне і фактично є недоступним для регіональних ресурсів. Контрзаходи, спеціалізовані на захисті менших та середніх ресурсів, отримали менший розвиток через поширеність великомасштабних атак у минулому і, таким чином, нині відстають від розвитку самих DDoS-атак. Для протидії кібератакам необхідний комплекс заходів із захисту інформаційних систем, даних та інфраструктури від несанкціонованих вторгнень, пошкоджень чи використання.

[1]. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2017). Retrieved from http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf [in English].

[2]. Ramaseri Chandra, A. N., El Jamiy, F., & Reza, H. (2022). A systematic survey on cybersickness in virtual environments. Computers, 11(4), 51.

[3]. Keshavarz, B., Murovec, B., Mohanathas, N., & others. (2023). The visually induced motion sickness susceptibility questionnaire (VIMSSQ): Estimating individual susceptibility to motion sickness-like symptoms when using visual devices. Human Factors, 65(1), 107–124.