Таким чином, економіка знань відіграє важливу роль у забезпеченні національної безпеки, але потребує балансування різних інтересів та врахування можливих ризиків. Підтримка інновацій, захист інтелектуальної власності, забезпечення наукової свободи та міжнародне співробітництво є ключовими елементами стратегії забезпечення національної безпеки у сфері економіки знань. Реалізація ефективних заходів у цих сферах дозволить країнам максимізувати користь від розвитку знань та інновацій, мінімізуючи при цьому можливі загрози та ризики.

1. Хамініч С.Ю. Основні тренди освіти в системі економіки знань // Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки». 2023. №5. https://doi.org/10.25313/2520-2294-2023-5-8886.

2. Khaminich S., Heti K. (2023), The knowledge economy as a factor for enterprise development in management system. *Philosophy, Economics and Law Review*. Volume 3, no. 1, 103-115. DOI: 10.31733/2786-491x-2023-1-103-115.

3. Kovalenko-Marchenkova Y. (2022). Management of the national economy as an element of the socio-economic space of the country. *Philosophy, Economics and Law Review*. Volume 6, no. 3, 30-37. DOI: 10.31520/2616-7107/2022.6.3-4.

УДК 004.056.57
DOI: 10.31733/15-03-2024/2/313-315

Андрій ГРЕБЕНЮК
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

DDoS АТАКИ В УКРАЇНІ:ВИКЛИКИ ТА ДОКУМЕНТУВАННЯ ЗАГРОЗ

У сучасному цифровому світі, де залежність від технологій надто велика, інтернет-простір стає ареною для різноманітних кіберзагроз. Однією з таких загроз є атаки типу DDoS (розподілені атаки на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам), які в Україні виявилися особливо проблематичними. Це явище не тільки порушує безпеку в Інтернеті, але і викликає серйозні наслідки для українського суспільства та економіки. Однією з основних проблем, пов'язаних з DDoS атаками, є їх розподіленість і широка масштабність. Кіберзлочинці використовують ботнети для організації атак, що робить важким визначення точного джерела нападу. Україна, будучи цифрово розвиненою країною, стала привабливою мішенню для таких атак підчас військової агресії близького сусіда. Захист від DDoS атак в Україні став питанням національної безпеки.

Захист від DDoS атак в Україні є надзвичайно важливою задачею для бізнесу, урядових організацій та інших важливих інфраструктурних об'єктів. Нижче подано кілька ключових стратегій та заходів для захисту від DDoS атак:

– Встановлення систем моніторингу та ідентифікації аномалій, які можуть вказувати на DDoS атаку. Використання спеціалізованих програм та апаратних засобів для виявлення надмірної активності.

– Застосування фільтрів на рівні мережі для блокування небажаних пакетів. Використання пристроїв із вбудованими системами фільтрації DDoS-трафіку.

– Встановлення та оновлення відповідного програмного забезпечення для виявлення та захисту від DDoS атак.

– Використання веб-файрволів та веб-безпеки для фільтрації та блокування небажаних трафіку.

– Забезпечення еластичності і масштабованості мережевої інфраструктури для можливості реагування на збільшену активність. Використовувати запасні інтернет-канали для перехоплення трафіку у разі атаки та забезпечення безперервності послуг.

– Використання хмарних служб захисту від DDoS, які можуть фільтрувати трафік

до того, як він потрапить до внутрішньої мережі. Хмарні рішення мають значні ресурси для ефективної фільтрації та виявлення атак.

– Проведення тренувань та навчання персоналу стосовно реагування на DDoS атаки. Визначення планів відновлення роботи в разі виявлення атаки.

– Укладення угод з постачальниками інтернет-послуг для реагування на DDoS атаки. Використання антиспуфінгу для зменшення ризику підробки джерела трафіку. [1]

Загальний підхід до захисту від DDoS атак включає в себе комбінацію технічних, організаційних та процедурних заходів. Постійне оновлення та аудит систем безпеки є ключовим елементом ефективного захисту від цих загроз.

Завдяки динаміці кіберзагроз, захист українських компанії та організації від DDoS атак вимагає постійного вдосконалення кіберзахисту та готовності до реагування на нові загрози. Співпраця між бізнесом, урядом та кіберзахисними експертами є ключем до успішної боротьби з цими атаками.

Розслідування DDoS атаки включає в себе кілька кроків, які мають на меті визначення джерела атаки, виявлення її характеристик та розроблення заходів для подальшого захисту.

Які можливо представити таким чином:

– Спостереження та виявлення;
– Визначте IP-адреси або групи IP-адрес;
– Визначення типу та характеристик атаки;
– Розуміння мети атаки;
– Знаходження та збереження доказів;
– Звіт та аналіз слабких місць;
– Запобігання подальших загроз.

Дії правоохоронних органів під час DDoS атак включають в себе кілька етапів, спрямованих на виявлення, зупинення та притягнення винних до відповідальності. Ось основні кроки, які правоохоронні органи можуть вживати в разі DDoS атаки [2]:

– Співпраця з інформаційними та кіберзахисними службами для визначення обсягу атаки та розгляду технічних характеристик. Вивчення можливої мети та мотивацій атаки.

– Звертання до постачальників інтернет-послуг для отримання інформації про джерело атаки та інші технічні деталі.

– Тісна співпраця з експертами в галузі кіберзахисту для аналізу атаки та розроблення заходів для її припинення.

– Оформлення судових постанов для отримання дозволу на втручання в інфраструктуру, яка використовується для запуску DDoS атаки.

– Детальний аналіз «логів» серверів, мережевих пристроїв та інших джерел інформації для визначення методів та інструментів, які використовувалися в атаках.

– Застосування технічних засобів для ідентифікації та фільтрації шкідливого трафіку.

– Визначення осіб чи організацій, які стоять за DDoS атакою. Припинення атак та притягнення винних осіб до відповідальності.

– Передача матеріалів до суду та участь у судових процедурах для притягнення винних до відповідальності.

– Забезпечення засобів та заходів для запобігання майбутнім DDoS атакам.

Важливо взаємодіяти із фахівцями кіберзахисту, інформаційними службами та постачальниками інтернет-послуг для успішного розслідування та припинення DDoS атак. Покарання винних може включати адміністративні санкції, кримінальні впровадження та інші судові заходи.

Уряд та компанії повинні співпрацювати для розробки та впровадження ефективних стратегій кіберзахисту. Потрібно збільшити свідомість громадськості та бізнес-сектору про загрози та заходи захисту. Також важливо розглядати співпрацю на міжнародному рівні. Україна повинна активно взаємодіяти з іншими країнами та міжнародними організаціями для обміну інформацією та вивчення кращих практик у сфері кіберзахисту. Розробка та впровадження комплексних заходів з кіберзахисту є вирішальними для забезпечення стабільності та безпеки в цифровому віці.

---

1. Краснобрижий І.В. Види та методики реалізації DoS та DDoS атак на державні автоматизовані системи, а також можливі шляхи боротьби з ними / І.В. Краснобрижий // Економічна та інформаційна безпека: проблеми та перспективи: матеріали Всеукр. наук.-практ. конф. (м. Дніпро, 14 квітня 2017 р.). Дніпро: ДДУВС, 2017. С. 89-94

2. З технічного боку. Як компаніям захиститися від DDoS-атак: пояснюють кіберексперти https://forbes.ua/company/s-tekhnicheskoy-storony-kak-kompaniyam-zashchititsya-ot-ddos-atak-obyasnyayut-kibereksperty-17022022-3733

3. Богданович В.Ю., Ворович Б.О., Марко Є.І. Інформаційна безпека як основа воєнної безпеки держави та суспільства. URL : http://znp-cvsd.nuou.org.ua/article/download/168924/168736/372345.

УДК 355.451
DOI: 10.31733/15-03-2024/2/315-317

Тетяна ЄЛОВА
докторант за спеціальністю
052 Політологія Волинського
національного університету
імені Лесі Українки,
кандидат політичних наук

СТРАТЕГІЧНІ КОМУНІКАЦІЇ В ОФІЦІЙНИХ ДОКУМЕНТАХ УКРАЇНИ

У сучасному світі, де інформація є ключовим ресурсом, стратегічні комунікації відіграють вирішальну роль у формуванні усвідомлених рішень, сприяють впливу на суспільство та визначають ефективність взаємодії між різними суб'єктами. Розглянемо сутність стратегічних комунікацій, їх важливість у сучасному світі та вплив на різні аспекти життя. По-перше, важливо зрозуміти, що стратегічні комунікації – це комплексний підхід до обміну інформацією, спрямований на досягнення конкретних цілей та вирішення стратегічних завдань. Вони базуються на вивченні аудиторії, розробці ефективних повідомлень та використанні різноманітних каналів комунікації.

З одного боку, стратегічні комунікації впливають на політичні процеси, формуючи громадську думку та визначаючи ставлення суспільства до різних подій та питань. Наприклад, під час виборчих кампаній політичні партії та кандидати активно використовують стратегічні комунікації для просування своїх ідей та залучення виборців. З іншого боку, стратегічні комунікації мають велике значення в бізнесі та управлінні. Компанії використовують їх для побудови позитивного образу бренду, залучення нових клієнтів та управління кризовими ситуаціями. Ефективне використання стратегічних комунікацій дозволяє підвищити конкурентоспроможність підприємства та забезпечити його стійкий розвиток.

Окрім того, стратегічні комунікації впливають і на міжнародні відносини. Країни та міжнародні організації використовують їх для підтримки своїх позицій у міжнародному співтоваристві, залучення підтримки інших країн та партнерів та вирішення глобальних проблем.

Створення та впровадження системи стратегічних комунікацій у секторі безпеки і оборони України визначається Указом Президента від 14 березня 2016 р. № 92/2016 «Про рішення Ради національної безпеки і оборони України від 4 березня 2016 р. «Про Концепцію розвитку сектору безпеки і оборони України»« [5], Концепцією стратегічних комунікацій Міністерства оборони України та Збройних Сил України, яка була затверджена наказом Міністерства оборони України від 22.11.2017 р. № 612. У документі зазначено, що «узгоджене та своєчасне застосування стратегічних комунікацій має вирішальне значення у протистоянні загрозам в інформаційному просторі, стає джерелом активного розповсюдження інформації у засобах масової інформації та реагування на поширення неправдивої інформації» [4].

Відповідно до вимог НАТО щодо розвитку комунікаційної сфери, всі процеси повинні стати більш простими та швидкими. Це є ключовою умовою для того, щоб інформаційні та комунікаційні аспекти стали основою всіх рівнів формування політики, планування та реалізації стратегічних комунікацій у Міністерстві оборони та Збройних Силах.

Значення стратегічних комунікацій особливо актуалізується у контексті забезпечення національної безпеки, формування національної ідеї та об'єднання громадян