Абзалов Денис Владиславович

курсант 2-го курсу факультету №3 Донецького державного університету внутрішніх справ

Габорець Ольга Андріївна

доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки, факультету №3 Донецького державного університету внутрішніх справ, доктор філософії, доцент

КІБЕРБЕЗПЕКА ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ ІНФОРМАЦІЇНОГО ЗАБЕЗПЕЧЕННЯ СЕКТОРУ ОБОРОНИ УКРАЇНИ

Кібербезпека є одним із ключових компонентів сучасної системи інформаційної безпеки, особливо в контексті обороноздатності держави. Для України, яка перебуває під постійним тиском кіберзагроз, ефективний кіберзахист відіграє критичну роль у забезпеченні національної безпеки та стійкості державних інституцій.

Кібербезпека визначається як стан захищеності життєво важливих інтересів особи, суспільства та держави у кіберпросторі. Її досягнення можливе завдяки системному впровадженню правових, організаційних та технічних заходів, спрямованих на мінімізацію ризиків, пов'язаних із використанням інформаційних технологій.

З початком повномасштабної агресії росії проти України кількість і масштаб кібератак суттєво зросли. Згідно з даними урядової команди CERT-UA, у другій половині 2023 року було зафіксовано та розслідувано 1,46 тисячі кіберінцидентів. Основними цілями атак стали міністерства, органи державної влади та об'єкти критичної інфраструктури. Зокрема, урядові організації зазнали атак 347 разів, місцеві органи влади – 276 разів, установи сектору безпеки та оборони – 175 разів, а комерційні організації – 127 разів. Особливу увагу хакери приділили енергетичному сектору (92 атаки), телекомунікаційному сектору (81 атака), освітнім закладам (38 атак), транспортній галузі (32 атаки) та фінансовому сектору (30 атак). Значні ризики також відчули IT-сектор (25 атак), засоби масової інформації (15 атак) і медичні установи (12 атак) [1].

Напередодні повномасштабного вторгнення, у січні 2022 року, кібератаки із застосуванням шкідливого програмного забезпечення, зокрема WhisperGate, завдали шкоди сайтам урядових установ України, зокрема Міністерству закордонних справ та Міністерству освіти. У жовтні 2022 року хакерська група Sandworm здійснила синхронізовану атаку на енергетичну систему України, поєднавши її з ракетними ударами, що призвело до пошкодження низки підстанцій.

Протягом війни активно використовувалися програми-вимагачі, такі як Caddy-Wiper і SwiftSlicer, метою яких було знищення даних. Масштабні DDoS-атаки, наприклад, на Київстар у грудні 2023 року, спричинили перебої у зв’язку для мільйонів користувачів. Додатково російські хакери застосовували методи дезінформації, включаючи злами медіа, поширення фейкових новин через соцмережі та фішингові розсилки [2].

Забезпечення кібербезпеки в Україні потребує комплексного підходу, який охоплює аспекти зазначені у Таблиці 1.

Отже, кібербезпека є фундаментальним компонентом інформаційної підтримки оборонного сектору України, особливо в умовах сучасних загроз, таких як кібертероризм, інформаційні війни та гібридні атаки. Надійний кіберзахист критично важливих

інфраструктур і військових систем забезпечує не лише збереження національної безпеки, але й ефективну адаптацію до зовнішніх викликів, що постають перед державою. З огляду на стрімкий розвиток технологій, постійне вдосконалення стратегій, методів та ресурсів кіберзахисту є ключовою умовою для забезпечення ефективності протидії кібератакам.

Табл 1. Забезпечення кібербезпеки в Україні

Категорія	**Результат**
Законодавство	Удосконалення нормативної бази відповідно до міжнародних стандартів (NIST, ISO 27001) та впровадження чіткої стратегії кібербезпеки.
Технології	Використання сучасних засобів захисту (шифрування, багаторівнева автентифікація), розробка національного ПЗ та систем моніторингу загроз.
Освіта	Підготовка фахівців через освітні програми й навчання, підвищення цифрової грамотності та регулярні симуляції для перевірки готовності до інцидентів.
Міжнародна співпраця	Участь у програмах NATO та міжнародних кібернавчаннях, обмін досвідом та інформацією про загрози.
Критична інфраструктура	Захист ключових секторів (енергетика, транспорт), впровадження резервних систем для безперервної роботи.
Боротьба з дезінформацією	Створення платформ для перевірки фактів, моніторинг та блокування шкідливих ресурсів.

Інтеграція заходів кібербезпеки з іншими складовими національної оборони створює потужну платформу для зміцнення безпеки держави. Важливо, щоб розвиток кібербезпеки розглядався як один із пріоритетів державної політики, оскільки саме він є вирішальним для забезпечення стабільності, стійкості та суверенітету України в умовах глобалізованого світу. Ефективне впровадження кіберзахисту стає не лише засобом протидії сучасним загрозам, а й важливим елементом формування технологічно оснащеної та адаптивної системи національної безпеки.

Література

1. Названа кількість кібератак в Україні за минулий рік. URL: https://www.slovoidilo.ua/2024/01/31/novyna/suspilstvo/nazvana-kilkist-kiberatak-ukrayini-mynulyj-rik
2. Гендиректор «Київстару»: IT – інфраструктура компанії частково зруйнована внаслідок хакерської атаки. URL: https://ms.detector.media/withoutsection/post/33724/2023-12-12-gendyrektor-kyivstaru-it-infrastruktura-kompanii-chastkovo-zruynovana-vnaslidok-khakerskoi-ataky/