УДК 004.056:327.5

Бабенко В.Г.
Черкаський державний технологічний університет

Основні групи кіберзброї та особливості її застосування

Зважаючи на те, що промисловість в Україні останніми роками характеризувалася занепадом, то логічно, що як в соціальній так і у військових сферах при виробництві електронної та радіотехнічної апаратури використовувалась здебільшого закордонна елементна база. Така ж ситуація характерна і для сектору розробки та впровадження програмного забезпечення у всіх сферах діяльності нашої країни. Це призвело до виникнення можливості здійснення кібератак, тобто надало можливість застосування кіберзброї проти військових, політичних, фінансово-економічних та промислових інфраструктур держави. А зважаючи на те, що масштаби завданих збитків в результаті кібератак є параметром, який можливо регулювати, то це означає, що кіберзброю можливо застосовувати як мехнізм тиску та терору [1]. Отже, в зв'язку із реальною загрозою застосування проти будь-якої держави, в тому числі і України, сучасної кіберзброї сьогодні виникла нагальна необхідність розвитку механізмів та засобів захисту кіберпростору як держави так і її громадян, а також забезпечення можливості використання кіберзброї у власних цілях, наприклад, для ведення оборонної кібервійни. Саме це спровокувало швидке відновлення та прискорення модернізації української високотехнологічної промисловості та виробництва власної елементної бази, яка здатна повністю забезпечити потреби оборонної сфери.

Сучасні військові конфлікти характеризуються багатовимірністю. Значну частку ефективних засобів ведення війни сьогодні почала займати саме кіберзброя різного призначення. За критерієм принципу дії кіберзброю можливо розділити на п'ять основних груп [2] (табл. 1).

Таблиця 1 – Основні групи кіберзброї

Механізм дії	Особливості застосування
Мережева кіберзброя	
Доставка багатофункціональних комп'ютерних програм до цілей з використанням різного роду мереж і, перш за все, Інтернету. Як правило, при застосуванні мережевої кіберзброї Інтернет виступає своєрідними воротами, що дозволяють потрапити в закриті, внутрішні військові і соціальні мережі, що включають критичні об'єкти.	Цей вид кіберзброї використовується для операцій проти політичних і військових командних і штабних об'єктів, а також ураження різного роду допоміжних і тилових структур, що включають і соціальні мережі.
Попередньо встановлена кіберзброя	
Попередньо встановлене керуюче програмне забезпечення в елементну базу, яке з великою ймовірністю містить різного роду «логічні бомби», «закладки» і т.п. Вони приводяться в дію за допомогою сигналів, які передаються допоміжними програмними кодами, і виводять з ладу озброєння, на яких встановлені відповідні апаратні блоки.	Можливість доступу до ІТ-ринку держави, до якої буде застосовуватися дана група кіберзброї. Побудова на базі мікропроцесорів та інших електронних компонентів закордонного виробництва військових кіберпристроїв, які вмонтовані в високотехнологічне, автоматизоване та роботизоване озброєння.

Механізм дії	Особливості застосування
Проникаюча кіберзброя	
Як правило, цілеспрямована зміна акустичного, оптичного та інших середовищ з відповідною модифікацією сигналів, що надходять на зовнішні сенсорні датчики високотехнологічної зброї. За допомогою цих впливів забезпечуються перебої в роботі бойової техніки, яка атакує, або повне знищення керуючих комп'ютеризованих блоків цієї техніки.	Відсутність необхідності для доставки кіберзброї наявності мереж або каналів зв'язку між оператором і бойовою технікою, що атакує.
Електромагнітна зброя	
Характеризується різним радіусом дії, повністю виводить з ладу бойову техніку, де встановлені бортові комп'ютери, авіоніка і інші комп'ютеризовані блоки. В результаті дії цього типу зброї відповідна елементна база, яка базується, перш за все, на кремнієвій складовій, повністю виводиться з ладу, що називається, «випалюється».	Даний тип озброєнь відноситься до наступальних озброєнь і передбачає нанесення превентивного удару на стадії розгортання бойових підрозділів у ході конфлікту.
Комунікаційна кіберзброя	
Всі автоматизовані і велика частина роботизованих озброєнь підтримують постійну комунікацію з зовнішніми операторами. Відповідно, даний вид кіберзброї є програмний код, що спотворює, блокує і підміняє обмін сигналами між віддаленим оператором і бойовим автоматизованим або роботизованим пристроєм.	Завдяки цьому виду озброєнь може бути здійснено як руйнування об'єкта, так і перехоплення управління.

Відмінною рисою новітньої військової техніки є її автоматизація або роботизація. На основі аналізу сучасних військових конфліктів виявлено, що одними із найвідоміших прикладів автоматизованих бойових або розвідувальних машин можна назвати безпілотні літальні апарати (дрони) [3]. Так як їх застосування передбачає дистанційне управління оператором, то перспективним є розвиток комунікаційної кіберзброї. Ще однією причиною для її розвитку є збільшення чисельності повністю роботизованої бойової техніки, яка має в своїй структурі автономний блок управління з вбудованим програмним забезпеченням. Також одним із перспективних напрямів розвитку кіберзброї є створення інтегрованих людино-комп’ютерних систем, таких як, наприклад, екзоскелети для спецпідрозділів [2].

Підводячи підсумки, робимо висновки, що при викликах сьогодення кожна країна повинна мати сучасні засоби захисту від кібернетичних загроз, а також обов’язково забезпечити сучасною кіберзброєї і власну армію.

Список використаних джерел

1. *Новые технологии - новое оружие: [Електронний ресурс]. – Режим доступу:* http://antivirus.ua/content/novye-tehnologii-novoe-oruzhie.
2. *Кибероружие: пятое измерение современной войны: [Електронний ресурс]. – Режим доступу:* http://army-news.ru/2013/12/kiberoruzhiepyatoe-izmerenie-sovremennoj-vojny/
3. *115 ідей застосування дронів: [Електронний ресурс]. – Режим доступу:* http://startupline.com.ua/social/how-to-use-drones.