МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
УКРАЇНИ "КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ
ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"

НАВЧАЛЬНО-НАУКОВИЙ
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

THEORETICAL AND APPLIED CYBERSECURITY

Перша Всеукраїнська
науково-практична конференція,
присвячена 100-річному ювілею
академіка В.М. Глушкова

Матеріали конференції

Київ – 2023

потенційних векторів атаки. Зокрема, методи "знизу вверх" та "сценарний" дозволяють розглядати проблеми з різних перспектив, хоча кожен з них має свої переваги та обмеження.

Типові сценарії атаки в Kubernetes, такі як підвищення привілеїв, відмова в обслуговуванні, виконання шкідливого коду, криптоджекінг, зловживання шкідливими контейнерами та використання ресурсів, вимагають вдумливого розгляду в контексті дерева атак.

Відносно специфіки моделювання загроз для Kubernetes, слід зауважити важливість забезпечення глибокого розуміння архітектури Kubernetes, механізмів аутентифікації та авторизації, мережевих політик та інших компонентів системи. На основі цієї інформації, можна ідентифікувати активи, пріоритезувати ризики та розробити стратегії для їх зменшення.

Перелік використаних джерел

1. Bobbio A. A methodology for qualitative/quantitative analysis of weighted attack trees / A. Bobbio, L. Egidi, R. Terruggia. // IFAC Proceedings Volumes. – 2013. – №46. – С. 133.
2. Containers Matrix [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://attack.mitre.org/matrices/enterprise/containers/.
3. Threat Matrix for Kubernetes [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://microsoft.github.io/Threat-Matrix-for-Kubernetes/

КОМПЛЕКС І СИНЕРГІЯ КІБЕРДІЙ У СУЧАСНИХ КОНФЛІКТАХ

Даник Ю.[1], Ланде Д.[1], Шестаков В.[2]

[1] Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського”, м. Київ, Україна

[2] Національна академія Служби безпеки України, м. Київ, Україна

Анотація. У доповіді розглянуто окремі види кібердій як складових кібер операції. Показано, що синергія кібердій відбувається у разі їх комплексного застосування за єдиним замислом, узгодженими за місцем та часом реалізації.
Ключові слова: кібердії, кібероборона, кібербезпека, ризики, технології конфліктів і війни.

Вступ

Конфлікти сучасності стають комплексним протиборством різних технологій, у тому числі, інформаційних. При цьому, значна роль досі належить використанню форм, способів і засобів збройної боротьби війн попередньої епохи [1]. Однак стійкою світовою тенденцією є перенесення протиборства в кіберпростір [2].

Сторони конфлікту здійснюють потужні кіберінформаційні дії. Так, протягом 2022 року за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було зареєстровано в 2,8 разів більше кіберінцидентів, ніж в 2021 році, геолокація джерел яких асоційована з росією збільшилась на 26% [3]. Відзначається, що з початку вторгнення рф в Україні активно розвивається громадянський кіберсупротив. За координації фахівців суб'єктів кібербезпеки і кібероборони силами волонтерів та активістів громадянського суспільства шляхом комплексного і системного ведення за єдиним замислом і планом різноманітних, але, в першу чергу, інформаційних, інформаційно-психологічних, когнітивних та кібердій. реалізуються атаки, які спрямовані на: порушення систем управління державою та її сектором безпеки і оборони; дискредитацію ключових акторів та маніпуляцію репутацією, викривлення сприйняття осіб і дій військово-політичного керівництва держави особовим складом збройних сил, населенням та світовою спільнотою.

Водночас, однією з проблем функціонування сил оборони України в умовах існуючих та потенційних загроз є неспроможність ефективно реагувати на зростаючу кількість загроз у кіберпросторі [4].

Тому стає наукове протиріччя – розвиток інформаційних технологій спричиняє ускладнення інформаційних і кіберзагроз, веде до синергії різноманітних інформаційних та кібердій, що потребує пошуку шляхів адекватного реагування на такі загрози та зниження ризиків їх реалізації.

Метою доповіді є представлення ймовірного комплексу кібердій та можливий результат їх синергії, який може бути реалізовано у військових конфліктах сучасності.

Основний матеріал

Суттєвим стримуючим чинником на шляху комплексного вивчення синергії кібердій при їх взаємному впливі і взаємодії за їх паралельно-послідовного ведення за єдиним замислом і планом так і за їх відсутності в першу чергу виступає дефініційна невизначеність та відсутність таксономічної моделі. Базові поняття наведено в [5]. Тому далі розкривається авторське бачення сутності та змісту окремих категорій, показуються їх спільні та відмінні риси.

Дослідження показали, що, як правило, кібердії є комплексними, узгоджені з інформаційним, інформаційно-психологічними та когнітивними впливами, проводяться за єдиним замислом і планом у формі кібероперації [5, 6].

У доповіді розкривається сутність та описується найбільш ймовірний сценарій проведення кібероперації.

Доводиться, що операція в кіберпросторі складається з чотирьох основних компонентів: кіберпротиборство, кібероперація в мережах, операція з кіберпідтримки, операція з кіберобізнаності.

Обґрунтовується, що у багатьох випадках ефективність кібероперацій на порядок вище ефективності операцій із застосуванням засобів вогневого ураження або значно підвищує ефективність інших операцій. Високий показник ефективності кібероперації пояснюється тим, що сучасні засоби кібервійни досягли такого рівня бойових можливостей, який гарантує їм внесення радикальних змін у сутність збройного протиборства.

Враховується, що у визначеній зоні (районі) воєнних дій здійснюється формування з наявних засобів локального інформаційно-кібернетичного простору.

Обґрунтовується, що синергетичний ефект матиме місце тільки тоді, коли інформаційні та кібернетичні дії здійснюються за єдиним задумом і планом та узгоджуються за завданнями в часі та просторі.

У доповіді приведено приклади, кількісні і якісні оцінки синергії, урахування яких сприяє виробленню ефективних заходів кібероборони.

Висновки

За результатами досліджень можна стверджувати, що синергетичні ефекти виникають внаслідок взаємодії інформаційних та кібердій Розкрито типовий сценарій проведення кібероперації. Доведено, що синергетичний ефект матиме місце у випадку, коли інформаційні та кібердії реалізуються за єдиним задумом і планом, узгоджуються за завданнями в часі та просторі.

Показано, що завдання завчасного виявлення, оцінювання та прогнозування синергетичних ефектів вирішується на основі розробленої та розкритої в доповіді методології. Обґрунтовано, що розроблена методологія виступає ефективним регулятором нелінійних процесів, які

виникають унаслідок взаємодії інформаційної та кібернетичної компонент.

Перелік використаних джерел

1. Danyk Yuriy, Shestakov Valery. Ways of reducing civilian casualties during wars and armed conflicts of modern times. High-tech aspects. The actual problems of the world today. London, 2019. Vol. 2. pp. 15 – 30.
2. Стратегія кібербезпеки України. Затверджено Указом Президента України від 26.08.2021 № 447/2021.
3. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. 2022. URL: https://scpc.gov.ua/api/docs/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1.pdf
4. Стратегічний оборонний бюлетень України. Затверджено Указом Президента України від 17.09.2021 №473/2021.
5. Даник Ю., Грищук Р., Основи кібернетичної безпеки : Монографія, за заг. ред. Ю. Г. Даника, Житомир: ЖНАЕУ, 2016, 636 с.
6. Даник Ю. Г., Грищук Р. В. Синергія інформаційних та кібернетичних дій // Труди університету. Київ, 2014. – № 6 (127). – С. 132–143.

МОДЕЛЮВАННЯ КІБЕРАТАК НА ЕНЕРГЕТИЧНІ СИСТЕМИ

Шрейдер М.О., Стьопочкіна І. В.
Фізико-технічний інститут,Київ, Україна Навчально-науковий Фізико-технічний інститут КПІ ім. Ігоря Сікорського, Київ, Україна

В роботі розглянуто модель системи автоматичного керування генерацією електроенергії в умовах існування кібернетичних впливів, які можуть призвести до наявності спотворення сигналів та їх затримки. Увагу зосереджено на

Наукове видання

ТЕОРЕТИЧНА ТА ПРИКЛАДНА КІБЕРБЕЗПЕКА

Перша Всеукраїнська
науково-практична конференція,
присвячена 100-річному ювілею
академіка В. М. Глушкова

Матеріали конференції

(Українською та англійською мовами)

В авторській редакції
Надруковано з оригінал-макета замовника

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Свідоцтво про державну реєстрацію: серія ДК № 5354 від 25.05.2017 р.
просп. Перемоги, 37,
м. Київ, 03056

Підп. до друку 09.05.2023. Формат 60 × 84 1/16. Папір офс. Гарнітура Times.
Спосіб друку – електрографічний. Ум. друк. арк. 15,58.
Обл.-вид. арк. 13,03. Наклад 100 пр. Поз. 23-3-3-004. Зам. № 23-061.

Видавництво «Політехніка» КПІ ім. Ігоря Сікорського
вул. Політехнічна, 14, корп. 15
м. Київ, 03056
тел. (044) 204-81-78