ЗБІРНИК ТЕЗ ДОПОВІДЕЙ — СПІЛЬНІ ДІЇ ВІЙСЬКОВИХ ФОРМУВАНЬ І ПРАВООХОРОННИХ ОРГАНІВ ДЕРЖАВИ: ПРОБЛЕМИ ТА ШЛЯХИ ВИРІШЕННЯ В УМОВАХ ВОЄННОГО СТАНУ

ВІЙСЬКОВА АКАДЕМІЯ (м. ОДЕСА)

СПІЛЬНІ ДІЇ ВІЙСЬКОВИХ ФОРМУВАНЬ І ПРАВООХОРОННИХ ОРГАНІВ ДЕРЖАВИ: ПРОБЛЕМИ ТА ШЛЯХИ ВИРІШЕННЯ В УМОВАХ ВОЄННОГО СТАНУ

Збірник тез доповідей
IV Міжнародної науково-практичної конференції

20 жовтня 2022 року

Військова академія (м. Одеса)

- Одеський державний університет внутрішніх справ
- Національна академія Національної гвардії України
- Кафедра військової підготовки Сумського державного університету
- Національна академія Державної прикордонної служби України імені Богдана Хмельницького
- Науково-дослідний центр Національної академії Національної гвардії України
- Академія Державної пенітенціарної служби
- Східне регіональне управління Державної прикордонної служби України
- Навчально-науковий інститут права та підготовки фахівців до підрозділів національної поліції
- Сумський державний університет
- Дніпропетровський державний університет внутрішніх справ
- Харківський національний університет внутрішніх справ
- Національний університет цивільного захисту України
- Одеський державний аграрний університет
- Львівський державний університет безпеки життєдіяльності
- Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки

IV МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

Сумський державний університет

20 жовтня 2022 року

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ 2022

СПІЛЬНІ ДІЇ ВІЙСЬКОВИХ ФОРМУВАНЬ І ПРАВООХОРОННИХ ОРГАНІВ ДЕРЖАВИ: ПРОБЛЕМИ ТА ШЛЯХИ ВИРІШЕННЯ В УМОВАХ ВОЄННОГО СТАНУ

Шановні учасники конференції!

Вчена рада Військової академії (м. Одеса) та організаційний комітет висловлює щирі слова вдячності за надіслані тези і безпосередню участь у конференції!

Вірю, що найближчим часом ми зможемо проводити конференції в офлайн-форматі, в тісному спілкуванні ділитися науковими думками і демонструвати практичні результати досліджень!

Бажаю всім перемоги та мирного неба над головою!

Слава Україні!

ВІЙСЬКОВА АКАДЕМІЯ (м. ОДЕСА)
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ
ім. БОГДАНА ХМЕЛЬНИЦЬКОГО (м. ХМЕЛЬНИЦЬКИЙ)
НАЦІОНАЛЬНА АКАДЕМІЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ (М. ХАРКІВ)

СПІЛЬНІ ДІЇ ВІЙСЬКОВИХ ФОРМУВАНЬ І ПРАВООХОРОННИХ ОРГАНІВ ДЕРЖАВИ: ПРОБЛЕМИ ТА ШЛЯХИ ВИРІШЕННЯ В УМОВАХ ВОЄННОГО СТАНУ

Збірник тез доповідей
IV Міжнародної науково-практичної конференції

20 жовтня 2022 року

м. Одеса

Пядишев Володимир, д-р юрид. наук, доц.
Дулгер Володимир, канд. юрид. наук
Одеський державний університет внутрішніх справ

ПРОТИДІЯ КІБЕРВІЙНІ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ: ВИСНОВКИ ЗАРУБІЖНИХ ФАХІВЦІВ

Перенесення інформаційних воєн у кіберпростір призвело до поєднання двох найнебезпечніших і найменш вивчених форм злочинності – кіберзлочинності та організованої злочинності. Дилема, як захиститися від них, стала ще серйознішою. Міжнародне
співтовариство уникало цього питання, і інформаційна війна повністю ігнорувалась. Проте, з розвитком війни, розв'язаної Російською Федерацією щодо України, ставлення світової спільноти до кібер-війни почало змінюватися. Нова ситуація змусила світову Інтернет-спільноту замислитися над такими геополітичними питаннями: 1) Яку роль має відігравати існуючий механізм управління Інтернетом в умовах воєнного стану? 2) З огляду на

жорстокість війни, чи існують цінності вищої сили, здатні вплинути на управління Інтернетом з огляду на його фундаментальний характер? 3) Які ефективні інструменти онлайн-спільнота використовує у всьому світі для досягнення консенсусу щодо онлайн-управління?

Сьогодні, у 2022 році експерти з Secureworld (приватного фонду, що діє на користь усіх народів) визначили сім національних цілей використання кіберзасобів: 1) спостереження та моніторинг домашніх груп; 2) зміцнення та вдосконалення національного кіберзахисту; 3) контроль та маніпулювання інформаційним середовищем; 4) збирання зовнішніх розвідданих для національної безпеки; 5) комерційна вигода чи прискорення зростання вітчизняної промисловості; 6) знищення або виведення з ладу інфраструктури та можливостей противника; 7) визначення міжнародних кібернорм та технічних стандартів.

У червні 2022 року експерти з Cyberpeaceinstitute (незалежна та нейтральна неурядова організація, місією якої є забезпечення прав людей на безпеку, гідність та справедливість у кіберпросторі) зазначили, що на полях битв 21 століття кібератаки змінюють способи ведення війни, про що свідчить війна в Україні. Атаки на критичну інфраструктуру вкрай руйнівні. Масштаби порушення кібербезпеки як засобу ведення війни безпрецедентні. Необхідні заходи для боротьби з погрозами у кіберпросторі сьогодні та в майбутньому.

Також у червні 2022 року експерти з InformationWeek (американського журналу з інформаційних технологій бізнесу) у статті «Передовий досвід кібербезпеки у війні в Україні» зазначають, що кібер-засоби стали зброєю війни. Всі компанії повинні знати кожну одиницю обладнання, якою вони володіють: чи є вона частиною обладнання, яке вони придбали, чи щось вороже. Вони також повинні мати дуже надійний режим виправлення вразливостей. Щомісяця вони повинні сканувати вразливості у своїй системі, а потім виправляти їх. Повинна використовуватися багатофакторна автентифікація, а не простий пароль.

Кіберфахівці НАТО виділяють 7 типів кібератак: *шпигунство* – спостереження за іншими країнами з метою крадіжки та подальшого використання їх секретів; *саботаж* – ворожі уряди чи терористи можуть вкрасти інформацію, знищити її чи використати внутрішні загрози; *атаки типу «відмова в обслуговуванні» (DoS)* – для порушення критичних операцій та систем, а також для блокування доступу до конфіденційних веб-сайтів цивільних осіб, військових та співробітників служби безпеки чи дослідницьких організацій; *атаки на електричну мережу* дозволяють відключити критично важливі системи, порушити інфраструктуру, зв'язок та потенційно завдати інших ушкоджень; *пропагандистські атаки* – щоб люди втратили довіру до своєї країни або стали на бік ворогів; *економічний зрив* – зловмисники можуть націлюватися на комп'ютерні мережі економічних установ, щоб вкрасти гроші або заблокувати доступ людей до коштів; *раптові атаки* – аналог Перл-Харбор та 11 вересня – масована несподівана гібридна атака може підготувати підґрунтя для фізичної атаки.

Кіберфахівці Європарламенту так визначають вплив кібератак на інфраструктуру України. З 24 лютого обмежені російські кібератаки порушили розподіл ліків, продуктів харчування та предметів першої потреби. Їх вплив варіювався від запобігання доступу до основних послуг до крадіжки даних та дезінформації, у тому числі з використанням технології дипфейку. Інша зловмисна кіберактивність включала відправку фішингових електронних листів, розподілені атаки типу «відмова в обслуговуванні» та використання шкідливих програм для знищення даних, бекдорів, програмного забезпечення для спостереження та викрадачів інформації.

Вони також свідчать про допомогу, яку світова спільнота прагне надавати Україні у протидії російським кібератакам. Ініціативи під керівництвом ЄС, США та НАТО були реалізовані з метою нейтралізації кіберзагроз та захисту основної інфраструктури. ЄС задіяв свої Групи швидкого реагування у кіберпросторі (проект у рамках Постійного структурованого співробітництва (PESCO) у сфері політики безпеки та оборони) для підтримки кіберзахисту України. Незалежними хакерами було зроблено значну кількість контратак, що торкнулися російської держави, системи безпеки, банківської системи та засобів масової інформації. Європарламент закликав посилити допомогу Україні в галузі кібербезпеки та повною мірою використати режими кіберсанкцій ЄС проти осіб, організацій та органів, причетних до різних кібератаків, спрямованих проти України.

Експерти з Центру аналізу європейської політики (CEPA) зазначають, що на початку війни Росії вдалося відключити супутниковий зв'язок України. Але українці швидко його відновили і енергетичні мережі країни, банки та інші вразливі об'єкти продовжували працювати.

Українські фахівці зазначають, що кіберпростір має стати інструментом асиметричної відповіді на агресію. Основними завданнями цієї відповіді мають бути: управління не лише своїми засобами, а й засобами супротивника; створення та вдосконалення інтелектуального потенціалу; проведення систематизованих тренувань з управління у кризових ситуаціях з охопленням всіх можливих варіантів розвитку подій для всіх органів та систем управління. Багаторівневий захист може використовуватися для вирішення завдань інформаційної безпеки об'єктів різного призначення, як для захисту самого об'єкта, так і для захисту інформації, що циркулює в ньому.