DOI:**10.33099/2311-7249/2019-34-1-95-102**

УДК: 044.056

Юрій Григорович Даник *(доктор технічних наук, професор)*

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ОСОБЛИВОСТІ СТВОРЕННЯ КІБЕРПОЛІГОНІВ ДЛЯ ДОСЛІДЖЕННЯ КОМПЛЕКСНИХ КІБЕРДІЙ ТА ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

Для ефективного виконання комплексу заходів забезпечення інформаційної і кібербезпеки в кіберпросторі з відпрацюванням заходів протидії гібридним впливам запропоновано створення кіберполігонів, які надають можливість дослідження комплексних кібердій та підготовки фахівців з кібербезпеки. Запропоновано методику здійснення розробки методологічного забезпечення для моделювання на кіберполігоні процесів моніторингу, аналітичної обробки інформації, прогнозування, планування і здійснення заходів пасивної та активної протидії інформаційним і кіберзагрозам в кіберпросторі. Запропоновано забезпечувати врахування особливостей умов апріорної невизначеності, варіативність щільностей потоків деструктивних впливів та значної динаміки кризових ситуацій на основі застосування методів ситуаційного управління, фрактального аналізу, самоорганізації та біфуркаційних моделей. В статті розглянуто особливості застосування принципів ситуативного управління програмно-апаратним середовищем кіберполігону, на якому виконується комплекс заходів та процесів забезпечення інформаційної та кібер- безпеки в кіберпросторі та через кіберпростір. Ці процеси розглядаються як динамічні і циклічні, такі, що мають певну специфіку в залежності від розгляду конкретних кризових ситуацій на обраному переліку необхідних і достатніх елементів з доступних та наявних складових кіберполігону.

Ключові слова*: кіберполігон; кіберзагроза, кібербезпека; кіберінцидент; кіберпростір; кібероборона.*

Вступ

Дієві результати реалізації завдань аналізу та синтезу складних систем, автоматизованого збору, обробки і аналізу інформації в умовах апріорної невизначеності та високої щільності потоку деструктивних впливів і значної динаміки кризових ситуацій, забезпечує застосування синергетичних методів, зокрема методів ситуаційного управління, фрактального аналізу, самоорганізації, біфуркаційних моделей тощо. Впровадження принципів ситуативного управління надає можливості раціонального розподілу і перерозподілу власних ресурсів і концентрації зусиль на критичних для забезпечення безпеки напрямах дій супротивника. Методи фрактального аналізу, самоорганізації і біфуркаційні моделі дозволяють своєчасно виявити загрози та кризові ситуації, передбачити напрям їх розвитку і реальну спрямованість. На практиці це забезпечує підвищення ефективності заходів протидії інформаційним впливам завдяки випередженню противника у своєчасності, повноті та достовірності інформації, за часом реагування та у діях. Для реалізації цих підходів необхідною мірою є створення кіберполігонів.

Постановка проблеми. Реалії сьогодення доводять, що сучасні методи та способи реалізації гібридних впливів супроводжуються значним потоком динамічно змінюваних кризових ситуацій. Їм властива апріорна невизначеність за метою, суб'єктом та об'єктом впливу, змістом, сутністю і способами реалізації. Технологічно побудова відомих систем протидії таким кризовим ситуаціям, форми і способи їх застосування орієнтовані на формування статичної надмірної структури системи. Розподіл завдань між усіма складовими системи здійснюється рівномірно з вибірковістю елементів лише за їх призначенням. Збільшення кількості та щільності потоку кризових ситуацій, кіберінцидентів та їх типів відпрацьовується збільшенням елементів структури. Це породжує інформаційну надмірність даних та ускладнення їх передачі і обробки. На таких самих принципах побудовані програмні засоби реалізації процесів оперативного виявлення, захисту та активної протидії інформаційним загрозам в кіберпросторі. Такі підходи не є дієвими в реальних умовах обстановки, під час застосування противником переважаючих або рівних за складом та рівнем розвитку засобів інформаційного впливу і здійснення масованих інформаційних та кібератак, які супроводжуються іншими несиловими і силовими методами досягнення мети конфлікту.

Таким чином, має місце актуальна проблема створення кіберполігонів для дослідження комплексних кібердій та підготовки фахівців з кібербезпеки з метою виконання завдань щодо розробки методологічного забезпечення автоматизованого моніторингу, аналітичної обробки інформації, прогнозування, планування та здійснення заходів пасивної і активної протидій інформаційним загрозам в кіберпросторі. Її

© Ю.Г. Даник

вирішення та підвищення ефективності комплексу заходів забезпечення інформаційної та кібербезпеки в кіберпросторі з відпрацюванням заходів протидії гібридним впливам в цілому вимагає наявності методологічних основ створення та організації ефективного застосування відповідних кіберполігонов.

Аналіз останніх досліджень і публікацій. Проблематика розробки та впровадження лабораторних середовищ для відпрацювання дій в кіберпросторі здебільшого розвивається у створенні таких типів кіберполиігонів: університетського (типу кіберполігону KYPO Масарикового університету м. Брно, Чехія); частки цивільного (на прикладі рішень компанії Forward Defense, м. Абу-Дабі, ОАЕ); національного військового (кіберполігон National Cyber Range, м. Орландо, шт. Флоріда, США); міжнаціонального (кіберполігон НАТО, м. Таллінн, Естонія). Програмно-апаратні засоби вказаних кіберполігонів не мають своєю метою та функціонально і технічно не забезпечують проведення комплексних досліджень інформаційного впливу на технічну і ергатичну складову систем управління різного рівня та призначення. При цьому втрачається можливість дослідження синергетичного ефекту взаємного посилення інформаційно-психологічних і кібервпливів, які реалізуються та розвиваються в кіберпросторі.

Традиційні підходи до створення, як правило, обмежуються здебільшого дослідницькими функціями вивчення загроз суто кібернетичного напряму без урахування реального досвіду сучасних гібридних впливів, що знижує адекватність отримуваних результатів.

Метою статті є розробка методики створення кіберполігонів для дослідження комплексних кібердій в кіберпросторі і через кіберпростір з відпрацюванням заходів протидії гібридним кібервпливам та підготовки фахівців з кібербезпеки.

Виклад основного матеріалу дослідження

Розробка та створення кіберполігону для дослідження і багатостороннього відпрацювання заходів протидії гібридним впливам в кіберпросторі реалізується загальнонауковими методами теорії системного аналізу.

Методика створення кіберполігону для відпрацювання інноваційних засобів і заходів забезпечення інформаційної та кібербезпеки в кіберпросторі в умовах гібридних конфліктів різної інтенсивності і змісту, з відпрацюванням заходів протидії гібридним впливам базується на здійсненні комплексу наукових досліджень фундаментального і прикладного характеру, реалізації інженерних завдань і організаційно-технічних заходів, суть і зміст яких передбачає наступне:

1. удосконалення науково-прикладних та технологічних принципів побудови і реалізації програмно-апаратних засобів моніторингу кіберпростору, захисту та впливу, їх практична апробація;

2. розробку фундаментальних та прикладних принципів побудови математичного забезпечення програмно-апаратних засобів реалізації процесів моніторингу, аналітичної обробки інформації, прогнозування, планування та здійснення заходів пасивної і активної протидії інформаційним і кіберзагрозам в кіберпросторі;

3. розробку та практичну апробацію в середовищі кіберполігона програмних засобів реалізації процесів моніторингу, аналітичної обробки інформації, прогнозування, планування і здійснення заходів пасивної і активної протидії інформаційним і кіберзагрозам в кіберпросторі;

4. розвиток новітніх форм, способів та методів протидії кіберзагрозам, захисту критичних інфраструктур, суб'єктів та об'єктів органів управління сектору безпеки та оборони держави, суспільства і особи за допомогою реалізації комплексу заходів інформаційної безпеки в кіберпросторі в умовах гібридних конфліктів різної інтенсивності;

5. розробку методичних основ для класифікації, стандартизації та сертифікації кіберполігонів, а також створення системи класифікації і стандартів кіберполігонів.

Створення кіберполігонів для дослідження комплексних кібердій в кіберпросторі і через кіберпростір забезпечить формування основ для створення потужних регіональних кіберцентрів та залучення цих структур до цілодобового оперативного чергування в системі національної і загальноєвропейської інформаційної і кібербезпеки з використанням сил і засобів кіберполігону, відпрацьовання на ньому теоретичних та прикладних принципів побудови програмно-технічних засобів, форм і способів протидії гібридним впливам в кіберпросторі.

Кіберполігон – це сукупність програмно-апаратних засобів, об'єднаних єдиною розподіленою локальною мережею з виходом в Інтернет, що призначена для відпрацювання прикладних питань розробки, проектування та проведення випробувань програмно-технічних систем (комплексів) забезпечення інформаційної (інформаційно-психологічної) та кібербезпеки в ході реалізації функцій моніторингу, захисту та активних впливів, проведення багатосторонніх навчань, забезпечення узагальнення досвіду, розвитку форм, способів та методів прогнозування, запобігання, виявлення і протидії кризовим ситуаціям в кіберпросторі, здійснення заходів практичної підготовки, перепідготовки та підвищення кваліфікації військових (цивільних) фахівців (за національними стандартами та стандартами НАТО), а також для проведення фундаментальних та прикладних наукових досліджень у галузі інформаційної і кібербезпеки та кібероборони держави.

Спеціалізований комплексний кіберполігон створюється по ідеології відкритих, розподілених, складних, ергатичних інформаційно-управляючих

систем, інваріантних за своєю структурою та рівнем завдань. У його структурі та архітектурі передбачено впровадження технологій захищених комп'ютерних мереж зі стаціонарним та мобільним комплектами обладнання зі взаємозамінними, стандартизованими в межах цільових завдань модулями. В якості функціональної основи передбачено використання циклів управління: Critique – критика, Explore – дослідження, Observation - спостереження (збір інформації від внутрішніх та зовнішніх джерел); Processing – обробка, Compare – порівняння, Orient - орієнтування (формування декількох можливих планів дій з оцінкою кожного з них за векторами критеріїв); Decide - рішення (вибір найкращого плану дій для практичної реалізації); Act - дії (практична реалізація вибраного плану дій); Adapt – адаптація (Restructuring – реструктуризація). Це забезпечить впровадження моделі незалежного ситуативного управління з відпрацюванням в масштабі часу, близькому до реального, потоку кризових ситуацій.

Розробка та виготовлення діючих кіберполігонів здійснюється з базових дискретних компонентів. До складу кіберполігону входять два ідентичні за призначенням, складом, функціональними можливостями комплекти спеціалізованих програмно-апаратних комплексів:

комплект сил кібероборони;

комплект сил тестування на кіберзахищеність.

Комплект сил кібероборони призначений для забезпечення кібербезпеки сервісів та служб дата-центру кіберполігону, а також захисту його операторів від впливів на них через кіберпростір.

Комплект сил тестування на кіберзахищеність призначений для тестування сервісів та служб дата-центру кіберполігону, а також дослідження стійкості його операторів до інформаційних впливів через кіберпростір.

До складу кіберполігону включений об'єкт тестування, який являє собою потужний дата-центр, сервіси та служби якого, з одного боку, захищаються силами та засобами сил кібероборони, з іншої – тестуються на кіберзахищеність силами та засобами другого комплекту.

Окремі компоненти, загальні для двох комплектів, які входять до кіберполігону це:

кластер планування, організації і управління роботи кіберполігону;

кластер міжполігонної взаємодії;

підсистема забезпечення функціонування сервісів та служб дата-центра.

підсистема моделювання заходів та засобів кіберзахисту провідних і безпровідних мереж дата-центру;

підсистема моделювання заходів і засобів кіберзахисту системи управління, мережної (фізичної і логічної) топології, програмно-апаратного забезпечення сервісів та служб дата-центру;

підсистема моделювання технологій інформаційного захисту операторів дата-центру через кіберпростір;

підсистема моделювання технологій криптографічного захисту;

підсистема моделювання заходів, засобів і технологій захисту від інформаційних і кібернетичних впливів критичних елементів інфраструктури, суб'єктів і об'єктів органів управління сектора безпеки і оборони держави, суспільства і особи в умовах гібридних конфліктів різної інтенсивності;

підсистема моделювання та імітації дій в кіберпросторі, проведення навчань (тренувань) з кібербезпеки та кібероборони;

підсистема моделювання кібератак на криптосистеми дата-центру;

підсистема моделювання соціотехнічних кібератак через кіберпростір на операторів дата-центра, суб'єкти та об'єкти органів управління сектору безпеки та оборони держави, суспільства і особистості в умовах гібридних конфліктів різної інтенсивності;

підсистема тестування сервісів та служб дата-центра на кіберзахищеність.

В основу схеми мережної топології кіберполігону покладені комплекти, об'єкти, компоненти, кластери і підсистеми кіберполігону.

Розробка кожного базового дискретного компоненту може здійснюватися окремо, ізольовано або за загальними підходами з обміном результатів проектування. Об'єднання віддалених дискретних компонент здійснюється шляхом їх інформаційного об'єднання в єдине кіберсередовище, яке створене функціонально об'єднаними: внутрішнім (локальним), комбінованим (локально-глобальним) і зовнішнім (глобальним) кіберпростором. З технологічної точки зору таке функціонально-інформаційне об'єднання здійснюється на протокольних рівнях відповідного типу.

Запропонована структура повнофункціонального комплексного кіберполігону поступово, на трьох локально-глобальних рівнях кіберпростору, з нарощуванням можливостей забезпечує відпрацювання форм, способів, методів, алгоритмів, методик та технологій виявлення кібератак, заходів пасивної і активної протидії ним, ліквідації наслідків застосування кіберзброї та відновлення нормальних режимів функціонування мереж управління військами та зброєю, а також реалізацію комплексу заходів моніторингу і виявлення загроз, їх аналізу, прогнозування, планування здійснення активних та пасивних дій з протидії інформаційно-психологічним впливам в кіберпросторі та аналіз ефективності проведених заходів.

Програмно-апаратні ресурси підсистеми тестування на кіберзахищеність забезпечують можливість проведення кібервпливів різного типу, використовуючи відповідні мережні протоколи, вразливості системного та прикладного програмного забезпечення, недосконалості антивірусного програмного забезпечення. Наприклад: сканування портів, відмова в

обслуговуванні, прослуховування та перехоплення потоку інформації в каналах мережі, псевдосанкціоноване проникнення в підсистему захисту, знищення, спотворення, крадіжка інформації, блокування доступу до неї в підсистемі кібероборони за допомогою засобів спеціального програмного впливу тощо. Технічні пристрої і спеціалізоване програмне забезпечення повинні гарантувати надійний захист системних ресурсів та інформації, яка циркулює і зберігається на комп'ютерах в локальній мережі підсистеми кібероборони.

У рамках проекту фахівці з інформаційної безпеки (кожен окремо або у складі певних команд) зможуть відпрацьовувати спеціальні прийоми кібервпливів та захисту від них, не завдаючи реальної шкоди існуючій інформаційній інфраструктурі держави.

Структура повнофункціонального комплексного кіберполігону забезпечує одночасно автономне, багатостороннє та багаторівневе виконання цільових завдань відповідно до реальних умов.

Розробка і створення кіберполігонів вимагає вирішення таких часткових завдань:

удосконалення науково-прикладних і технологічних принципів побудови та реалізації програмно-апаратних засобів моніторингу кіберпростору, захисту і впливів для створення кіберполігону;

розробка структури та детальної архітектури кіберполігону відповідно до відомих науково-прикладних і технологічних принципів його побудови;

створення кіберполігону з двох базових його комплектів за схемою та архітектурою, забезпечення функціонування (налаштування, тестування) першого (локального) рівня кіберпростору відповідно до категорій декомпозиційного розподілу;

створення повнофункціонального комплексного кіберполігону шляхом інформаційного об'єднання створених дискретних компонентів в єдине інформаційне середовище, які функціонують і породжують внутрішню комбіновану (локально-глобальну) і зовнішню складову кіберпростору;

розробка програми і методики випробувань комплексного кіберполігону з повнофункціональною структурою та архітектурою;

проведення випробувань створеного кіберполігону, оцінювання результатів випробувань, коригування його структури і функціоналу, затвердження результатів випробувань.

З метою ефективного виконання комплексу заходів забезпечення інформаційної і кібербезпеки в кіберпросторі з відпрацюванням заходів протидії гібридним впливам передбачається введення принципів ситуативного управління програмно-апаратним середовищем кіберполігону, на якому виконується комплекс заходів та процесів забезпечення інформаційної безпеки в кіберпросторі. Ці процеси розглядаються як динамічні і циклічні, такі, що реалізовуються під конкретну кризову ситуацію на обраному переліку необхідних і достатніх елементів з доступних та наявних складових кіберполігону. Для цього створюється і послідовно-паралельно виконує завдання об'єднаних функціонально та інформаційно пов'язаних віртуальних підсистем – інформаційно-управляючих кластерів (ІУК). Такі ІУК ситуативно синтезуються для виявлення, локалізації і ліквідації конкретної кризової ситуації. Відмічене реалізується у формі ситуативного структурно-параметричного синтезу складної розподіленої інформаційно-управляючої системи. Фактично реалізується процес ситуативного управління структурою і параметрами кіберполігону. Така процедура забезпечує просторово-часове, структурне і функціональне рознесення завдань відпрацювання щільного потоку деструктивних впливів при значній динаміці кризових ситуацій. При цьому знижується розмірність часткових завдань обробки інформації і навантаження на канали передачі даних. В якості практичного результату маємо: ефективне реагування на щільний потік динамічно-змінюваних деструктивних впливів при значній динаміці кризових ситуацій з властивостями апріорної невизначеності суб'єктів та об'єктів впливу, змісту, суті та способу реалізації; виконання цільових завдань в масштабі часу, близькому до реального, і з високими показниками достовірності і повноти вихідної інформації.

Ефективне виконання завдань забезпечення інформаційної безпеці залежить від постійного проведення фундаментальних та прикладних наукових досліджень, в ході яких уточнюється концепція і технології ситуаційного управління структурою та параметрами програмно-апаратного середовища кіберполігону для ефективної реалізації комплексу заходів і процесів забезпечення інформаційної безпеки в кіберпросторі в умовах значної щільності потоку динамічно-змінюваних деструктивних впливів при високій динаміці кризових ситуацій, які характеризуються апріорною невизначеністю.

На кожному інформаційно-управляючому кластері відпрацьовуються:

методики кластерного пошуку і систематизації інформації про інформаційні загрози в кіберпросторі;

методики виявлення та ідентифікації кризових ситуацій в умовах щільного їх потоку і динаміки змін з впровадженням принципів самоорганізації;

методики автоматизованого оперативного і поглибленого інтегрального аналізу інформації моніторингу;

методики прогнозування розвитку кризових ситуацій і загроз в інформаційній сфері з використанням біфуркаційних моделей;

методологічні підходи до планування заходів протидії інформаційним загрозам в кіберпросторі

та оцінювання їх ефективності;

методологічні підходи побудови програмно-апаратних комплексів автоматизованого пасивного і активного інформаційного (інформаційно-психологічною) та кіберзахисту.

В ході виконання завдань щодо розробки фундаментальних та прикладних принципів побудови математичного забезпечення програмно-апаратних засобів реалізації процесів моніторингу, аналітичної обробки інформації, планування і здійснення заходів пасивної і активної протидії інформаційним загрозам в кіберпросторі напрацьовуються дані для розробки програмних засобів реалізації процесів моніторингу, аналітичної обробки інформації, планування і здійснення заходів пасивної і активної протидії інформаційним загрозам в кіберпросторі.

Суть виконання завдання щодо розробки і практичної апробації в середовищі кіберполігону програмних засобів реалізації процесів моніторингу, аналітичної обробки інформації, прогнозування, планування і здійснення заходів пасивної і активної протидії інформаційним загрозам в кіберпросторі полягає в розробці програмно-апаратних комплексів, набору програмних додатків, розрахункових програм, моделей тощо, заснованих на розроблених фундаментальних і прикладних принципах побудови математичного забезпечення програмно-апаратних засобів реалізації процесів моніторингу, аналітичної обробки інформації, планування і здійснення заходів пасивної і активної протидії інформаційним загрозам в кіберпросторі для ефективної протидії гібридним впливам, які забезпечують виконання завдань:

ситуативного управління структурою і параметрами програмно-апаратного середовища кіберполігону;

кластерного пошуку і систематизації інформації про інформаційні загрози в кіберпросторі;

виявлення та ідентифікація кризових ситуацій в умовах щільного потоку деструктивних впливів і значної динаміки зміни кризових ситуацій з впровадженням принципів самоорганізації;

автоматизованого оперативного і поглибленого інтегрального аналізу інформації моніторингу;

прогнозування розвитку кризових ситуацій і загроз в інформаційній сфері з використанням біфуркаційних моделей;

планування заходів протидії інформаційним загрозам в кіберпросторі і оцінювання їх ефективності;

кібернетичного впливу та захисту від несанкціонованого доступу до інформаційно-телекомунікаційних систем;

формування лабораторного середовища для проведення спецдосліджень у галузі технічних і програмних засобів кіберзахисту;

визначення оптимального способу нейтралізації загроз в кіберпросторі з урахуванням наявних апаратно-програмних засобів технічного захисту інформації;

моделювання процесів нападу і захисту інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури;

оцінювання рівня захищеності електронних ресурсів і апаратно-програмних засобів інформаційно-телекомунікаційних систем;

аналізу ефективності кібервпливу на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури протидіючої сторони.

Створення програмного забезпечення з вказаними функціями здійснюється з використанням технологій побудови інтелектуальних експертних систем, систем підтримки прийняття рішень, геоінформаційних систем на сучасних мовах, технологіях та в середовищах програмування високого рівня.

Практична реалізація вищезазначеного потребує:

комплектів програмно-апаратних комплексів, наборів програмних додатків, моделей тощо, які реалізують вищеперелічені функції з програмною документацією до них;

програм і методик випробувань розроблених комплектів програмно-апаратних комплексів, набору програмних додатків, моделей тощо, для застосування на різних рівнях кіберпростору;

моніторингу результатів випробувань розроблених комплектів програмно-апаратних комплексів, набору програмних додатків, моделей тощо, на першому і другому рівнях кіберпростору.

Завдання щодо розвитку новітніх форм, способів і методів протидії викликам і загрозам тероризму, захисту критичних інфраструктур, суспільства, керівництва держави та його сектору безпеки, особистості за допомогою реалізації комплексу заходів інформаційної безпеки в кіберпросторі, спрямованих на протидію гібридним впливам полягає в реалізації конкретних практичних завдань на програмно-апаратних засобах кіберполігону. При цьому використовується метод напівнатурного моделювання із застосуванням принципів і прийомів теорії ігор, реалізацією антагоністичного конфлікту між умовно протиборчими сторонами, які діють на своїх базових дискретних компонентах кіберполігону. Персонал для роботи на автоматизованих робочих місцях кіберполігону може бути сформований з науково-педагогічних працівників, вчених, ад’юнктів, курсантів та фахівців з військ. Залежно від цілей досліджень розробляються сценарії дій. Документування результатів діяльності кіберполігону, їх апостеріорний аналіз забезпечує вироблення новітніх форм, способів та методів протидії викликам і загрозам тероризму, захисту критичних інфраструктур, суспільства, державного і військового керівництва, конкретних осіб (рис. 1).

В результаті виконання цього завдання отримують:

методики і сценарії проведення багатосторонніх навчань на кіберполігоні з питань забезпечення інформаційної безпеки в кіберпросторі;

Рис. 1. Схема розробки новітніх форм, способів і методів протидії інформаційним загрозам в кіберпросторі

діючий комплект програмно-апаратного комплексу кіберполігону для комплексного відпрацювання питань інформаційної (інформаційно-психологічної) та кібербезпеки з можливостями його стандартизації і сертифікації;

методи і методики підготовки персоналу для систем забезпечення інформаційної і кібербезпеки, отримані персоналом знання і навички;

результати випробувань розроблених комплектів програмно-апаратних комплексів, набору програмних додатків, моделей кіберпростору в умовах, наближених до реального застосування;

новітні форми, способи та методи протидії викликам і загрозам тероризму, захисту критичних інфраструктур, суспільства, керівництва держави та його сектору безпеки, особистостей за допомогою реалізації комплексу заходів інформаційної безпеки в кіберпросторі, спрямованих на протидію гібридним впливам;

відпрацьовані теоретичні і прикладні принципи, програмно-технічна складова і висококваліфіковані фахівці стануть основою для створення потужного кіберцентру та залучення цієї структури до цілодобового оперативного чергування в системі національної і загальноєвропейської інформаційної і кібербезпеки.

Створення та практичне застосування комплексних кіберполігонів забезпечує: проведення на постійній основі багатосторонніх національних та міжнародних навчань з питань інформаційної і кібербезпеки з удосконаленням і виробленням нових способів протидії новим та прогнозованим загрозам, впровадження стандартів альянсу НАТО і досягнення взаємосумісності Збройних Сил України з країнами-членами НАТО у сфері інформаційної і кібербезпеки;

впровадження нових напрямів перспективних фундаментальних і прикладних наукових досліджень з використанням емерджентних властивостей діючого кіберполігону, в якому сполучені методи напівнатурного моделювання, принципи і прийоми теорії ігор, антагоністичного конфлікту спрямовані на інтегроване дослідження проблем забезпечення інформаційної (інформаційно-психологічної) та кібербезпеки в кіберпросторі для протидії гібридним впливам;

сприяння ефективному вирішенню наукових завдань і виконання дослідницьких функцій у сфері кібербезпеки;

вироблення рекомендацій відносно удосконалення змісту та методик підготовки, перепідготовки і підвищення кваліфікації військових та цивільних фахівців у галузі інформаційної і кібербезпеки в країнах-членах та країнах-партнерах альянсу за національними стандартами і стандартами НАТО.

Комплексні кіберполігони, принципово відрізняється від існуючих аналогів поєднанням досліджень інформаційного впливу на технічну та ергатичну складову систем управління різного рівня і призначення (держави, критичними об'єктами, військами і зброєю та інші) з урахуванням синергетичного ефекту взаємного посилення відмічених категорій впливів, гібридних дій, що реалізовуються та розвиваються в кіберпросторі.

Відмінність програмно-апаратної складової таких кіберполігонів полягає у впровадженні принципів ситуативного управління, фрактального аналізу, самоорганізації, біфуркаційних моделей, що забезпечує ефективне виконання завдань забезпечення інформаційної (інформаційно-психологічної) та кібербезпеки в умовах апріорної невизначеності, високої щільності потоку деструктивних впливів і значної динаміки кризових ситуацій в інформаційній сфері, характерній для сучасних гібридних конфліктів.

Висновки і перспективи подальших досліджень

Таким чином, реалізація визначених завдань дасть можливість підвищити ефективність

комплексу заходів по забезпеченню інформаційної і кібербезпеки в кіберпросторі з відпрацюванням заходів протидії гібридним впливам. Це досягається шляхом розробки та виготовлення діючого комплекту комплексного кіберполігону, що забезпечить відпрацювання на ньому багатосторонніх практичних заходів по виробленню новітніх форм і способів протидії викликам і загрозам тероризму, захисту критичних інфраструктур, суспільства, керівництва держави, особистості.

Застосування комплексних кіберполігонів, як середовища для моделювання та імітації реальних дій в кіберпросторі та через кіберпростір підвищує ефективність дослідження форм, способів і методів кібердій та відпрацювання заходів протидії інформаційним і кіберзагрозам та гібридним кібервпливам без втручання в існуючу інформаційну структуру держави, дозволяє комплексно враховувати синергію інформаційно-психологічних та кібервпливів без втручання в роботу бойових інформаційних систем.

Наявність таких кіберполігонів в військових закладах вищої освіти надасть можливість:

проведення з їх використанням кібернавчань та командно-штабних навчань і тренувань з елементами відпрацювання дій в умовах комплексних деструктивних інформаційних та кібер- впливів;

участі у багатосторонніх національних та міжнародних навчаннях, удосконалення системи підготовки, перепідготовки та підвищення кваліфікації військових фахівців у галузі інформаційної та кібербезпеки з впровадженням комплексних підходів і стандартів НАТО, розвитку науково-прикладних напрямів кібербезпеки та кібероборони.

Література

1. Даник Ю. Г., Грищук Р. В. Основи кібернетичної безпеки: монографія; за заг. ред. проф. Ю. Г. Даника. Житомир: ЖНАЕУ, 2016. 636 с. **2. Даник Ю. Г.** Особливості формування системи кібернетичної безпеки України в контексті розвитку системи кібернетичної безпеки провідних країн світу / Ю. Г. Даник, Ю. М. Супрунов // Труди університету. – К. : НУОУ. – 2011. – № 7(106).– С. 5–21. **3. Даник Ю. Г., Вдовенко С. Г.** Концептуальні напрями комплексного вирішення проблеми захисту інформації в системі скритого управління збройних сил. Сучасні інформаційні технології у сфері безпеки та оборони 2017. №2(29). С. 98–107. **4.** Основи захисту інформації підручник: Ю.Г.Даник, С.Г. Вдовенко, О.О. Писарчук та ін; Житомирський військовий інститут ім. Корольова, Житомир, 2015 р. **5. Y. Danyk, T. Maliarchuk, Kohreidz**e; *Hybrid War Technologies*, international scientific journal "Business-Engineering, Georgian Technical University, Georgian Academy of Engineering, pp. 49-56, 2017. http://dspace.nplg.gov.ge/bitstream/1234/237163/1/Biznes-Injineringi_2017_N1-2.pdf. **6. Y. Danyk, T. Maliarchuk, Ch. Briggs,** Hybrid War: High-tech, Information and Cyber Conflicts, Connections. The Quarterly Journal. vol. 16, no.2 2017, pp. 5–24. URL: http://www.jstor.org/stable/26326478. **7. Y. Danyk, S. Gudz,** Special operations for disruption of state and military control system. Security and Defence Quarterly, published by War Studies University, Warsaw, Poland. № 4(9). 2015. URL: https://securityanddefence.pl/resources/html/article/details?id=124640. (дата звернення 27.04.2018). **8. Y. Danyk** State Cyber Defense Formation and Development in Conditions of Hybrid Challenges and Threats. International Conference on Information and Telecommunication Technologies and Radio Electronics. September. 11-15, 2017. DOI: https://doi.org/10.1109/UkrMiCo.2017.8095427. (дата звернення 27.04.2018). **9. F.G. Hoffman,** Hybrid Warfare and Challenges, Joint Forces Quarterly 52, 2009. **10.B. Boyer,** Countering Hybrid Threats in Cyberspace. Cyber Defense Review. Vol. 2 Ed. 3, 2015. **11. S. Harris Cyberwar :** The Fifth Theater of War. 2014. **12. J. Suler,** The Online Disinhibition Effect. CyberPsychology and Behavior, №7, 2004. **13. A. Clarke Cyber War:** The Next Threat to National Security and What to Do About It by Richard – http://indianstrategicknowledgeonline.com /web/Cyber_War_-_The_Nex_Threat_to_National_Security_and_What_to_Do_About_It_(Richard_A_Clarke)_(2010).pdf, 2010. **14.** What Is Cyber Threat Intelligence , And Why You Need It. – https://blog.unloq.io/what-is-cyber-threat-intelligence-and-why-you-need-it-fd33e24954da. Jan 19, 2017. **15. Y.G. Danyk, Y.I. Katkov, M.F. Pichugin,** National security: avoiding of critical situations. Monograph: National University of Defense of Ukraine, Korolyov Zhytomyr Military Institute, Zhytomyr, 2006

ОСОБЕННОСТИ И ОСНОВНЫЕ ТРЕБОВАНИЯ ПРИ РАЗРАБОТКЕ И СОЗДАНИИ КИБЕРПОЛИГОНИВ

Юрий Григорьевич Даник *(доктор технических наук, профессор)*

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

Для эффективного выполнения комплекса мер по обеспечению информационной и кибербезопасности в киберпространстве с отработкой мер противодействия гибридным воздействиям предложено создание киберполигонов, которые предоставляют возможность исследования комплексных кибердий и подготовки специалистов по кибербезопасности. Предложена методика осуществления разработки методологического обеспечения для моделирования на киберполигоне процессов мониторинга, аналитической обработки информации, прогнозирования, планирования и осуществления мероприятий пассивной и активной противодействия информационным и киберугрозам в киберпространстве. Предложено обеспечивать учет особенностей условий априорной неопределенности, вариативность плотностей потоков деструктивных воздействий и значительной

динамики кризисных ситуаций на основе применения методов ситуационного управления, фрактального анализа, самоорганизации и бифуркационных моделей. В статье рассмотрены особенности применения принципов ситуационного управления программно-аппаратной средой киберполигона, на котором выполняется комплекс мероприятий и процессов обеспечения информационной и кибербезопасности в киберпространстве и через киберпространство. Эти процессы рассматриваются как динамические и циклические, имеющие определенную специфику в зависимости от рассмотрения конкретных кризисных ситуаций на выбранном перечне необходимых и достаточных элементов из доступных и имеющихся составляющих киберполигона.

Ключевые слова: *киберполигон; кибербезопасность; киберинцидент; киберпространство; кибероборона.*

FEATURES AND MAIN REQUIREMENTS FOR DEVELOPMENT AND CREATING CIBERPOLIGONS

Yurii Danyk (Doctor of Technical Science, Professor)

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

For the effective implementation of a set of measures to ensure information and cybernetic security in the cybernetic space with the development of measures to combat hybrid influences, the creation of cybernetic polygons that provide the opportunity to study complex cybernetic actions and training of cybernetic security specialists is proposed. The methodology of the development of methodological support for simulation on the cyber space of monitoring processes, analytical processing of information, forecasting, planning and implementation of passive and active counteraction to information and cybernetic threats in cybernetic space is proposed. It is proposed to take into account the features of the conditions of a priori uncertainty, the variability of the densities of flows of destructive influences and the significant dynamics of crisis situations, based on the application of situational control methods, fractal analysis, self-organization and bifurcation models. In the article the peculiarities of application of the principles of situational management of the software and hardware environment of the cybernetic polygon are considered, on which a set of measures and processes for ensuring information and cybernetic security in the cybernetic space and through cybernetic space is carried out. These processes are considered as dynamic and cyclic, having certain specifics, depending on the consideration of specific crisis situations in the selected list of necessary and sufficient elements from available and available components of the cybernetic site.

Key words: *cyber renge; cyber security; cybernetic incident; cybernetic space; cyber defense.*

References

1. Danyk Y. H., Hryshchuk R. V. Osnovy kibernetychnoyi bezpeky: monohrafiya; za zah. red. prof. YU. H. Danyka. Zhytomyr: ZHNAEU, 2016. 636 p. **2. Danyk Y. H.** Osoblyvosti formuvannya systemy kibernetychnoyi bezpeky Ukrayiny v konteksti rozvytku systemy kibernetychnoyi bezpeky providnykh krayin svitu / Y. H. Danyk, Y. M. Suprunov // Trudy universytetu. – K. : NUOU. – 2011. – № 7(106).– S. 5–21. **3. Danyk Y. H., Vdovenko S. H.** Kontseptual′ni napryamy kompleksnoho vyrishennya problemy zakhystu informatsiyi v systemi skrytoho upravlinnya zbroynykh syl. Suchasni informatsiyni tekhnolohiyi u sferi bezpeky ta oborony 2017. №2(29). S. 98–107. **4.** Fundamentals of information protection – Textbook : Y.G.Danyk, S.G. Vdovenko, O.O. Pysarchuk and others; Korolyov Zhytomyr Military Institute, Zhytomyr, 2015. **5. Y. Danyk, T. Maliarchuk, Kohreidz**e; *Hybrid War Technologies*, international scientific journal "Business-Engineering, Georgian Technical University, Georgian Academy of Engineering, pp. 49-56, 2017. http://dspace.nplg.gov.ge/bitstream/1234/237163/1/Biznes-Injineringi_2017_N1-2.pdf. **6. Y. Danyk, T. Maliarchuk, Ch. Briggs,** Hybrid War: High-tech, Information and Cyber Conflicts, Connections. The Quarterly Journal. vol. 16, no.2 2017, pp. 5–24. URL: http://www.jstor.org/stable/26326478. **7. Y. Danyk, S. Gudz,** Special operations for disruption of state and military control system. Security and Defence Quarterly, published by War Studies University, Warsaw, Poland. № 4(9). 2015. URL: https://securityanddefence.pl/resources/html/article/details?id=124640. (дата звернення 27.04.2018). **8. Y. Danyk** State Cyber Defense Formation and Development in Conditions of Hybrid Challenges and Threats. International Conference on Information and Telecommunication Technologies and Radio Electronics. September. 11-15, 2017. DOI: https://doi.org/10.1109/UkrMiCo.2017.8095427. (дата звернення 27.04.2018). **9. F.G. Hoffman,** Hybrid Warfare and Challenges, Joint Forces Quarterly 52, 2009. **10.B. Boyer,** Countering Hybrid Threats in Cyberspace. Cyber Defense Review. Vol. 2 Ed. 3, 2015. **11. S. Harris Cyberwar :** The Fifth Theater of War. 2014. **12. J. Suler,** The Online Disinhibition Effect. CyberPsychology and Behavior, №7, 2004. **13. A. Clarke Cyber War:** The Next Threat to National Security and What to Do About It by Richard – http://indianstrategicknowledgeonline.com /web/Cyber_War_-_The_Nex_Threat_to_National_Security_and_What_to_Do_About_It_(Richard_A_Clarke)_(2010).pdf, 2010. **14.** What Is Cyber Threat Intelligence , And Why You Need It. – https://blog.unloq.io/what-is-cyber-threat-intelligence-and-why-you-need-it-fd33e24954da. Jan 19, 2017. **15. Y.G. Danyk, Y.I. Katkov, M.F. Pichugin,** National security: avoiding of critical situations. Monograph: National University of Defense of Ukraine, Korolyov Zhytomyr Military Institute, Zhytomyr, 2006