**«Нові методи і моделі систем виявлення кібертерористичних атак»**

***Основні наукові результати***

Основним результатом виконаної роботи є підвищення безпеки ресурсів інформаційних систем в умовах надзвичайного стану, породженого кібертерористичними діями в багатофакторному слабоформалізованому нечітко визначеному кіберсередовищі за допомогою, запропонованих відповідних принципів протидії, класифікації кібератак, політики дій щодо захисту інформаційних ресурсів та розроблених методів і моделей систем виявлення аномалій породжених атакуючими діями. У цьому зв'язку були отримані наступні результати.

1. Розроблена відповідна термінологія та класифікація кібертерористичних атак, визначено їх характерні ознаки, що дозволяє сформувати множини їх складових і таким чином формалізувати декларативні можливості відомих систем протидії і дозволить підвищити ефективність формування до них вимог при нових розробках засобів захисту та підвищення ефективності вибору існуючих засобів протидії.

2. Узагальнено класифікацію ключових складових характерних ознак функцій належності нечітких чисел, яка дозволяє на основі формалізованих груп нечітких величин підвищити ефективність процесу вибору сумісних методів теорії нечіткості для розв'язання широкого спектору прикладних задач у галузі захисту інформації.

3. Досліджено використання відомих методів, моделей, методологій, систем та інших спеціальних засобів нечітких множин щодо можливостей вирішення задач захисту від кібертерористичних атак та їх дієвість і ефективність при вирішенні задач експертного оцінювання у сфері технічного захисту інформації.

4. Запропоновано загальний підхід до формування нечітких моделей виявлення кібертерористичних атак (який включає: формування джерела даних; визначення набору нечітких параметрів; побудови нечітких еталонів; формування поточних нечітких значень; генерації нечітких евристичних правил; визначення значення параметра рівня аномального стану), який визначає узагальнену процедуру для побудови систем ідентифікації атак в умовах нечіткості.

5. Розроблена модель формування нечітких еталонів та модель з евристичними правилами і нечіткими арифметичними операціями які склали основу технології побудови систем ідентифікації атак за аномальним станом нечітко визначеного слабоформалізованого кіберсередовища.

6. Запропоновано структуру типової системи ідентифікації кібератак та на основі побудованих нечітких алгоритмів і моделей розроблено програмне забезпечення експериментальної системи виявлення сканування портів та проведено її верифікацію.

7. Розроблено рекомендації щодо організаційних заходів для захисту цивільної авіації від кіберзагроз на основі запропонованої класифікації кібератак. Рекомендації стали основою відповідного розділу DOC 30 ECAC.

***Практична цінність***

Результати роботи можуть бути використані при створенні політики комплексної системи протидії загрозам важливій інформації в умовах надзвичайного стану та формування методики виявлення кібертерористичних дій на створенні нових Стандартів та Рекомендованої практики ІСАО, захисту ресурсів інформаційних систем від кібертероризму та при створенні єдиних стандартів у сфері захисту ресурсів інформаційних систем щодо боротьби із кібертероризмом та в навчальному процесі для галузі знань 1701 "Інформаційна безпека".

**Перелік основних наукових публікацій, доповідей на конференціях, семінарах**

1. Кулик Н.С.Энциклопедия безопасности авиации/Корченко А.Г., Харченко В.П. та ін.. // К.: Техника.- 2008. – 1000 с.

2. Корченко О.Г. Захист інформації в мережах передачі даних ((Гриф МОН України. Лист № 1.4/18.Г-1 від 08.01.09 р.)). Навч. пос. / О.К. Юдін, Г.Ф. Конахович // К.: Вид-во ТОВ «НВП»ІНТЕРСЕРВІС», 2009. – 716 с.

3. Корченко О.Г. Нормативно-правове забезпечення інформаційної безпеки: Зб. Нормативно-правових документів / Дрейс Ю.О.// Житомир: ЖВІ НАУ, 2010. – 280 с.

4. Навчально-методичний комплекс «Програмні методи та засоби захисту інформації» CD “Віртуальний університет”, word 97, Windows 2000, http://www.nau.edu. ua /izn , К.: ТОВ “ЕЛЬВІК”, 2009.

5. Дисертація: М.В. Захарова «Синтез механізмів захисту інформаційних ресурсів від кібератак» 28.10.2010

6. Корченко О.Г. Можливості методу кореляції для аналізу сигналів тривоги від систем виявлення вторгнень/ Волянська В.В.// Тез.доп. наук.-техн. семінару «Проблеми інформатизації». – Черкаси:ЧДТУ.- 2008. – С. 7–8.

7. Корченко О.Г. Вплив загроз безпеки інформації на компоненти інформаційної системи/ Захарова М.В., Гришко Ю.М.// Тез.доп. наук.-техн. семінару «Проблеми інформатизації». – Черкаси:ЧДТУ.- 2008. – С. 20.

8. Корченко А.Г. Атаки на ресурсы информационных систем в современном обществе/ Рындюк В.А., Тулинцев В.Е., Пуха Д.А.// Мат. І междунар. научн.-практ. конф. “Информационные технологии в гуманитарном обществе”. – П.: ПГЛУ.- 2008. – Ч.2. – С. 224–233.

9. Корченко О.Г. Методологія синтезу механізмів захисту інформаційних ресурсів/ Паціра Є.В., Захарова М.В.// Сб. науч. тр. «Защита информации». – Спец. вип. – К.: НАУ.– 2008. – С.99–103.

10. Корченко О.Г. Криптографічний спосіб перетворення інформації побудований на шифрі Файстеля./ Паціра Є.В., Гнатюк С.О., Кінзерявий В.М.// «АВІА-2009»: матеріали ІХ міжнародної науково-технічної конференції. - Т.1. - К. : НАУ, 2009. - С. 2.17-2.20.

11. Корченко О.Г. Спосіб шифрування інформації на основі шифру Файстеля./ Паціра Є.В., Гнатюк С.О., Кінзерявий В.М. // Вісник інженерної академії України.-№2, 2009.-С. 117-121.

12. Корченко О.Г. Нечітке моделювання лінгвістичної змінної «Інформація» за змістом відомостей та видом операцій, що виконуються над нею/ Ю.О. Дрейс // Зб. наук. пр. «Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем». – Спец. вип.–Ж.: ЖВІ НАУ– 2009. - Вип. 2. –С.102–108.

13. Корченко А.Г. Методические основы экономики информационной безопасности/ Карпенко С.В., Гнатюк С.А.// Вісник Інженерної академії України. – 2009. №3-4. С.86-90.

14. Корченко А.Г. Развитие услуг по обеспечению информационной безопасности и их структура/ Карпенко С.В., Гнатюк С.А.// Вісник Інженерної академії України. – 2009. №3-4. С.91-95.

15. Є.В. Паціра Синтез механізмів захисту інформаційних ресурсів / М.В. Захарова, В.В. Волянська// Зб. тез.доп. міжвідом. наук.-практ. конф. «Сучасні проблеми захисту інформації з обмеженим доступом». – К:НАУ, 2009. – С. 51–52.

16. О.Г. Корченко Методологія синтезу механізмів захисту інформаційних ресурсів / О.Г. Корченко, М.В. Захарова, Є.В. Паціра // Защита информации: Сб. науч. тр. НАУ – Спец. вип. – К.: НАУ.– 2009. – С.99–103.

17. Харченко В.П.Кибертерроризм на авиационном транспорте./ Чеботаренко Ю.Б., Корченко А.Г., Пацира Е.В., Гнатюк С.А.// Проблеми інформатизації та управління: збірник наукових праць: Випуск 4 (28). – К. : НАУ, 2009. – С. 131–140.

18. Корченко О.Г., Паціра Є.В., Гнатюк С.О, Кінзерявий В.М., Казмірчук С.В. Ознаковий принцип формування класифікацій кібератак. Вісник Східноукраїнського національного університету імені Володимира Даля – №4 (146) – Ч. 1, 2010. – С. 184–193.

19. Корченко А.Г. Анализ и определение понятия риска для его интерпретации в области информационной безопасности / Пацира Е.В., Казмирчук С.В.// Журн. «Захист інформації». – Вип. №3 (48). – К.: ДУІКТ.– 2010. – С.5-10.