

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0219U100974

Державний реєстраційний номер: 0118U006133

Особливі позначки: відкрита

Дата реєстрації: 12-04-2019

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Система виявлення атак в локальних безпроводних мережах підприємств та їх об'єднань на основі технологій інтелектуального аналізу даних

Початок етапу: 07.2018

Закінчення етапу: 02.2019

Вид звітнього документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, 11, м. Хмельницький, Хмельницький р-н., Хмельницька обл., 29016, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 0975546925

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Товариство з обмеженою відповідальністю "Блок Майстер Україна"

Код за ЄДРПОУ: 36387055

Місцезнаходження: , м. Хмельницький, Хмельницький р-н., Хмельницька обл., 31104, Україна

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: (03854) 413 00

VI. Джерела, напрями та обсяги фінансування ДіР

Підстава для проведення ДіР: 52 - договір з вітчизняною організацією (органами місцевої ради, фондом, асоціацією, концерном тощо)

Напрямок фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

7722 - кошти підприємств, установ, організацій України

Фактичний обсяг фінансування (тис. грн.): 5

VII. Відомості про ДіР

Назва роботи українською:

Система виявлення атак в локальних безпроводних мережах підприємств та їх об'єднань на основі технологій інтелектуального аналізу даних

Назва роботи англійською:

System of detection of attacks in local wireless networks of enterprises and their associations on the basis of technologies of intellectual data analysis

Реферат українською:

Об'єкт дослідження - система виявлення атак через бездротову локальну мережу організації. Метою дослідження є підвищення ефективності виявлення атак через бездротову локальну мережу організації шляхом розробки моделей і алгоритмів вирішення даного завдання на основі технологій інтелектуального аналізу даних. Методи дослідження. У процесі дослідження використовувалися методи теорії графів, нейронних мереж, метод опорних векторів, метод k-найближчих сусідів, дерева прийняття рішень. Для оцінки ефективності пропонувані рішень застосовувалися методи функціонального, інформаційного та імітаційного моделювання. Запропонований метод виявлення атак в бездротовій мережі на основі класифікуючої моделі з використанням методів інтелектуального аналізу даних, що на відміну від існуючих методів дозволяє підвищити точність виявлення атак і знизити кількість помилкових спрацьовувань. За результатами проведених в навантажувальній мережі тестів, також розроблена методика по виявленню вразливих атакам скриптів і модулів в системах управління вмістом і подальшої оптимізації. Архітектура інтелектуальної системи виявлення бездротових атак функціонує на основі розроблених алгоритмів виявлення атак і їх об'єднання в ансамбль, застосування яких дозволяє з більш високою точністю і повнотою виявляти і блокувати атаки на бездротовий компонент інформаційної системи. Розроблено програмне забезпечення дослідницького прототипу інтелектуальної системи виявлення бездротових атак. Ефективність розробленого прототипу підтверджена методом імітаційного моделювання атак на сегмент локальної бездротової мережі організації з використанням реального мережевого трафіку. Прототип забезпечує підвищення на 15 : 18% точності виявлення атак на бездротовий компонент інформаційної системи

Реферат англійською:

The object of research is the system of detection of attacks through the wireless local area network of the organization. The purpose of the study is to increase the effectiveness of detecting attacks through the wireless local area network of the organization by developing models and algorithms for solving this problem on the basis of intelligent data analysis technologies. Research methods. In the process of research, methods of theory of graphs, neural networks, the method of reference vectors, the method of k-nearest neighbors, decision trees are used. Methods for functional, informational and simulation modeling were used to evaluate the effectiveness of the proposed solutions. The proposed method of detecting attacks in the wireless network based on the classifying model using the methods of data mining, which, unlike existing methods, can increase the accuracy of detection of attacks and reduce the number of false positives. According to the results of tests carried out in the loading network, a technique is also developed for identifying vulnerable script and module attacks in content management systems and further optimization. The architecture of the intelligent detection system for wireless attacks operates on the basis of developed algorithms for detecting attacks and their integration into an ensemble, the application of which allows more precise and complete detection and blocking of attacks on the wireless component of the information system. The software of the research prototype of the intelligent system of detecting wireless attacks has been developed. The effectiveness of the developed prototype is confirmed by the simulation simulation of attacks on the segment of the local wireless network of the organization using real network traffic. The prototype provides an increase of 15 : 18% accuracy of detection of attacks on the wireless

component of the information system

Індекс УДК: 004.7.03; 004.73, 004.73:004.45

Коди тематичних рубрик: 50.39.21

Керівники роботи

Власне Прізвище Ім'я По-батькові: Джулій Володимир Миколайович

Науковий ступінь:

Вчене звання:

Ідентифікатор ORCID ID:

Додаткова інформація:

VIII. Наукова (науково-технічна) продукція (НТП)

Назва НТП українською: Методика виявлення атак в локальних безпроводних мережах підприємств та їх об'єднань

Назва НТП англійською: Method of detection of attacks in local wireless networks of enterprises and their associations

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: підвищення точності виявлення атак

Галузь застосування: 72.19

Реєстраційний номер картки технології:

Опис НТП: Дослідження моделі атак в безпроводних мережах підприємств дозволило створити методику раннього виявлення та протидії атакам середньої і малої інтенсивності. Методика є універсальною, враховує, як регіональні особливості, так і інші фактори, і може бути застосована для виявлення і протидії атакам різних типів і різної потужності. Комплекс системних моделей деталізують процес виявлення атак і дозволяють інтегрувати систему з компонентами захисту інформації в організації з урахуванням вимог нормативних документів. Запропонована методика виявлення атак в бездротовій мережі на основі застосування класифікуючої моделі з використанням методів інтелектуального аналізу даних, яка на відміну від існуючих методів виявлення атак дозволяє підвищити точність виявлення атак і знизити кількість помилкових спрацьовувань за рахунок попереднього навчання і донавчання системи на даних реального мережевого трафіку. Отримана методика протестована на реальних даних. Для легітимних запитів повнота виявлення склали 0,9991 при точності 0,9811, для не легітимних запитів, повнота 0,9975, точність 0,9924. Прототип забезпечує підвищення від 15 до 18 % точності виявлення атак на бездротовий компонент інформаційної системи

Соціально-економічна спрямованість НТП: Забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг, Захист інформації в організаціях

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 01.2019

Закінчення етапу: 02.2019

Споживачі продукції: Товариство з обмеженою відповідальністю "Блок Майстер Україна"

Перспективні ринки: Підприємства та організації України

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи: Права не надаються

Наявність бізнес-плану: Ні

Техніко-економічне обґрунтування: Ні

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

IX. Бібліографічний опис

- 1 Джулій В. М. Моделі та алгоритми виявлення атак в бездротових мережах передачі даних / В. М. Джулій, О. С. Ленков, Л. О. Ряба // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – Київ : ВІКНУ, 2018. – Вип. 59. – С. 76-87.
- 2 Інтегральний критерій оцінки методів тестування додатків для мобільних пристроїв / В. М. Джулій, В. О. Браун, К. А. Кизима, Д. О. Селюков, Л. В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – Київ : ВІКНУ, 2018. – Вип. 61. – С. 40-49.
- 3 Джулій В. М. Метод виявлення та протидії розподіленим атакам, спрямованим на відмову в обслуговуванні / В. М. Джулій, О. О. Савіцька, В. Чорненький // Вісник Хмельницького національного університету. Технічні науки. – Хмельницький : ХНУ, 2019. – № 1. – С. 117-125.
- 4 Джулій В. М. Модель оцінки ймовірно-часових характеристик інформаційної взаємодії в мережі інтернет речей / В. М. Джулій, Б. М. Кізюн, І. В. Муляр // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – Київ : ВІКНУ, 2019. – Вип. 63. – С. 51-60.
- 5 Джулій В. М. Модель формування цілей інформаційного забезпечення підтримки процесів надання знань / В. М. Джулій, І. В. Гурман, А. А. Маковей // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – Київ : ВІКНУ, 2019. – Вип. 63. – С. 90-98.

X. Заключні відомості

Керівник юридичної особи

Войнаренко Михайло Петрович
д. е. н., 08.00.05

Перелік осіб-виконавців

Джулій Володимир Миколайович
Красильников Сергій Романович
(к. т. н.)
Огневий Олександр Вікторович
(к. т. н.)

**Відповідальний за підготовку
облікових документів**

Першина Л. І.

Телефон

+38 (097) 508-72-32

Реєстратор

**Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності**

