ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

Лойко О. П., Липовий А. Ю. , Шувалова Л. А.
Черкаський державний технологічний університет, Черкаси, Україна

Одним з напрямків захисту інформації в комп'ютерних мережах є технічний захист інформації (ТЗІ). У свою чергу, питання ТЗІ включають в себе захист інформації від несанкціонованого доступу (НСД) і захист інформації від витоку технічними каналами. Під НСД звичайно мається на увазі доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розглядаються канали сторонніх електромагнітних випромінювань і наведень, акустичні канали, оптичні канали та ін. [1].

Для захисту інформації від НСД на рівні прикладного й системного ПЗ нами використовуються системи розмежування доступу до інформації, системи ідентифікації й аутентифікации, системи антивірусного захисту. Для захисту інформації на рівні апаратного забезпечення використовуються апаратні ключі, системи сигналізації, засоби блокування пристроїв і інтерфейсів вводу-виводу інформації.

Розглядаються питання дослідження та синтезу, а також організації безпечного функціонування комп'ютерної мережі. Предметом досліджень є комп'ютерна мережа та її система безпеки. Об'єктом досліджень є організація безпечного середовища функціонування комп'ютерної мережі. Мета дослідження полягає в синтезі системи управління безпекою комп'ютерної мережі із застосуванням комплексних заходів і засобів. Для досягнення поставленої мети проведено аналіз стандартів і архітектур комп'ютерних систем, аналіз математичних моделей безпеки, здійснено вибір і реалізовано обґрунтовану систему заходів по забезпеченню безпеки мережі, а також виконано її синтез. Для створення засобів захисту інформації визначено загрози, форми та шляхи їх можливого прояву і здійснення в мережі.

Список літератури

1. Комп'ютерні мережі: Навчальний посібник / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. — Львів: «Магнолія 2006», 2013. — 256 с.

2. Andrew S. Tanenbaum, «Computer Networks (Hardcover)», Prentice Hall PTR., Published: August 9, 2002., Pages: 912., Edition: 4.

3. P. V. Kucherniuk, "Metody i tekhnolohii zakhystu komp'iuternykh merezh (fizychnyi ta kanalnyirivni) [Methods and technologies for computer networks protection (the physical and data link layers)]," Microsystems, Electron. Acoust., vol. 22, no. 6, pp. 64–70, 2017, DOI: 10.20535/2523-4455.2017.22.6.113191.

ВЕРИФІКАЦІЯ ВЕБ-САЙТУ НА ОСНОВІ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ СЕМАНТИЧНОГО ЯДРА

Тарасенко Я. В., Передеренко Д. М., Дмитренко С. С., Мушинська А. А.
Черкаський державний технологічний університет, Черкаси, Україна

Сьогодні веб-технології розповсюджені в усіх сферах діяльності. Однак, існують загрози фінансовому благополуччю окремих громадян і національній безпеці держави, як, наприклад, використання фішингових веб-сайтів з метою шахрайства, дезінформації чи пропаганди. Визначення автентичності веб-сайту є важливою та актуальною задачею. Існуючі технології можуть виявляти небезпечний протокол http, перевіряти відповідність сертифікату, а онлайн-сервіси дозволяють визначати фішингові веб-сайти. Однак, ці підходи не є ефективним при застосуванні технологій соціальної інженерії. При цьому, мало наукових робіт присвячено перевірці автентичності веб-сайту. Так, в наявних роботах перевірка автентичності здійснюється шляхом перевірки сертифіката з використанням мережевих протоколів [1] чи на основі асоціативної класифікації [2], що не завжди достатньо в поточних реаліях.

Метою доповіді є формування альтернативного підходу визначення автентичності веб-сайту та його контенту, що дозволить підвищити ефективність протидії фішинговим атакам. У доповіді наводяться результати дослідження веб-ресурсів з метою розробки альтернативного підходу визначення їх автентичності. Проведено аналіз різнонаправлених елементів типового веб-сайту та зроблено висновок про можливість використання семантичного ядра в якості контейнеру для впровадження унікальної мітки, оскільки наявні програмно-інструментальні засоби не можуть визначити складові елементи семантичного ядра незнайомого веб-сайту зі стовідсотковою точністю. В той же час, мітку ядра незнайомого веб-сайту зі стовідсотковою точністю пропонується створювати, впроваджувати та перевіряти на основі стеганографічних методів вбудовування цифрових водяних знаків. При цьому, висловлюється гіпотеза про можливість застосування в даному випадку квантово-семантичної лінгвістичної стеганографії, вперше описаної в [3]. Надається прогноз ефективності використання розробленого альтернативного підходу.

Список літератури

1. Магомедкеримова Г. З. Способы защиты данных в web -приложениях с применением ssl/tls протокола. *Информационные технологии в экономике и управлении. Сборник научных трудов ФГБОУ ВО «ДГТУ».* 2017. С. 62–69.

2. Abdelhamid N., Ayesh A., Thabtah F. Phishing detection based Associative Classification data mining. *Expert Systems with Applications.* 2014. Volume 41, Issue 13. P. 5948-5959. 2019. Т. 25, № 2. С. 96-103. DOI: https://doi.org/10.1016/j.eswa.2014.03.019

3. Тарасенко Я. В. Забезпечення надійності функціонування комп'ютерних лінгвістичних стегосистем в умовах протидії інфомраційній пропаганді. *Безпека інформації.* 2019. Т. 25, № 3. С. 174-181. DOI: https://doi.org/10.18372/2225-5036.25.13958