Авторська довідка

(кваліфікаційної роботи бакалавра)

Назва кваліфікаційної роботи бакалавра *Дослідження криптографічних протоколів захисту інформації в мережі Інтернет*
назви записувати нижнім регістром (як у реченні)

Назва (англ.): Research on cryptographic information protection protocols in the Internet
переклад англійською

Освітній ступінь : бакалавр

Шифр та назва спеціальності: 125 «Кібербезпека»
напр.:151 Автоматизація та комп'ютерно-інтегровані технології

Екзаменаційна комісія: Екзаменаційна комісія № 40
напр.: Екзаменаційна комісія №1

Установа захисту: Тернопільський національний технічний університет імені Івана Пулюя
напр.: Тернопільський національний технічний університет імені Івана Пулюя

Дата захисту: 20 червня 2023 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок роботи: 63

УДК:

Автор роботи
Прізвище, ім'я, по батькові (укр.): Костюк Катерина Олегівна
розкривати ініціали

Прізвище, ім'я (англ.): Kateryna Kostiuk Olehivna
використовувати паспортну транслітерацію (КМУ 2010)

Місце навчання (установа, факультет, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра кібербезпеки, м.Тернопіль, Україна

Керівник
Прізвище, ім'я, по батькові (укр.): Загородна Наталія Володимирівна
повністю

Прізвище, ім'я (англ.): Natalia Zagorodna Volodymyrivna
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Україна

Вчене звання, науковий ступінь, посада: кандидат технічних наук, доцент кафедри кібербезпеки

Рецензент
Прізвище, ім'я, по батькові (укр.): Никитюк В'ячеслав В'ячеславович
повністю

Прізвище, ім'я (англ.): Nikityuk Vyacheslav Vyacheslavovich
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, м.Тернопіль, Україна
Вчене звання, науковий ступінь, посада: кандидат технічних наук, доцент кафедри КН

Ключові слова:
українською: криптографія, криптографічні протоколи, шифрування, вразливості, мережа інтернет, конфіденційність, вебсервер
до 10 слів

англійською: cryptography, cryptographic protocols, encryption, vulnerabilities, internet, confidentiality, web server
до 10 слів

Анотація

українською:

Метою даної роботи є детальний аналіз, порівняння та оцінка криптографічних протоколів захисту інформації в мережі Інтернет, що дасть можливість виявити їх переваги та недоліки, а також потенційні вразливості.

Об’єкт дослідження – криптографічні протоколи захисту інформації в мережі Інтернет.

Предмет дослідження – алгоритми захисту інформації в криптографічних Інтернет-протоколах, виявлення та усунення вразливостей протоколів.

В кваліфікаційній роботі проведено порівняння криптографічних примітивів, аналіз криптографічних алгоритмів, порівняння криптографічних протоколів захисту в мережі Інтернет та їх версій, оцінка стану безпеки вебсервера, аналіз та усунення виявлених вразливостей вебсервера, що пов’язані з підтримкою небезпечних версій криптографічних протоколів SSL/TLS.

Результатом роботи є виявлення та усунення вразливостей вебсервера, пов’язаних підтримкою небезпечних версій криптографічних Інтернет-протоколів.

Для реалізації даної роботи були використані такі програмні продукти: VMware Workstation Pro, Tenable Nessus Vulnerability Scanner, Draw.io.

англійською:

The purpose of this work is a detailed analysis, comparison, and evaluation of cryptographic information protection protocols in the Internet, which will allow identifying their advantages, disadvantages, and potential vulnerabilities.

The object of research is cryptographic information protection protocols in the Internet.

The subject of research is information protection algorithms in cryptographic Internet protocols, detection and elimination of protocol vulnerabilities.

In the qualification work, a comparison of cryptographic primitives is conducted, cryptographic algorithms are analyzed, comparison of cryptographic protection protocols in the Internet and their versions is performed, the security state of a web server is evaluated, and identified vulnerabilities related to the support of insecure versions of SSL/TLS cryptographic protocols in the web server are analyzed and eliminated.

The result of the work is the detection and elimination of vulnerabilities in the web server related to the support of insecure versions of cryptographic Internet protocols.

The following software products were used for the implementation of this work: VMware Workstation Pro, Tenable Nessus Vulnerability Scanner, Draw.io.

Костюк К. О. Дослідження криптографічних протоколів захисту інформації в мережі Інтернет: кваліфікаційна робота бакалавра за спеціальністю 125 — Кібербезпека / К. О. Костюк. – Тернопіль: ТНТУ, 2023. – 63 с.