

Харківський національний університет радіоелектроніки

Кафедра електронних обчислювальних машин

БАГАТОШАРОВА ВІРТУАЛЬНА МЕРЕЖА

Виконав:
ст. групи КІУКІз-16-1
Яковенко К.О.

Керівник:
к.т.н., доц. Ткачов В.М.

АКТУАЛЬНІСТЬ ВИКОРИСТАННЯ ВІРТУАЛЬНИХ МЕРЕЖ

- виключення прослуховування трафіку у мережі;
- розблокування міжнародних бібліотек з обмеженим доступом;
- безпечне підключення до всіх Wi-Fi точок;
- приховане реальне географічне розташування.

ПОСТАНОВКА ЗАДАЧІ

Метою атестаційної роботи є розробка багат шарової віртуальної мережі для безпечної передачі даних у глобальних комп'ютерних мережах.

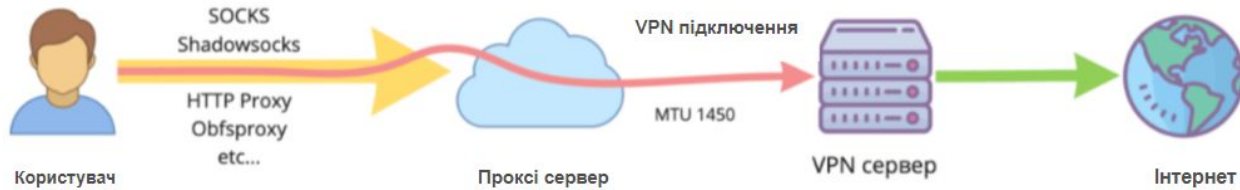
Для вирішення цієї задачі, в роботі вирішуються такі часткові задачі:

- аналіз особливостей функціонування існуючих віртуальних комп'ютерних мереж;
- розробка способу побудови віртуальної мережі;
- дослідження створеної мережі на предмет часових затримок при передачі даних.

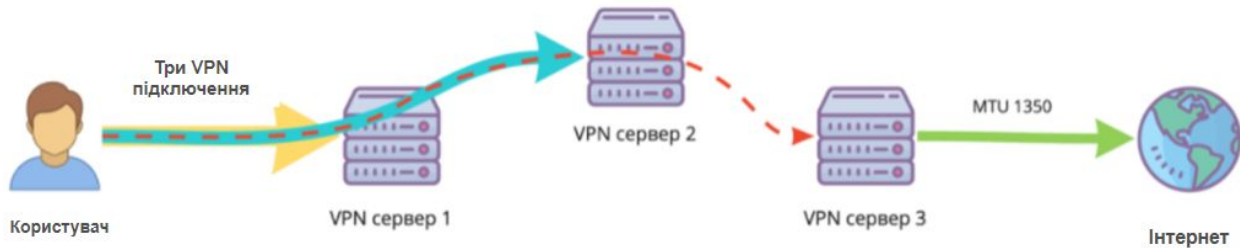
ОГЛЯД ІСНУЮЧИХ РІШЕНЬ



Демонстрація роботи VPN між серверами

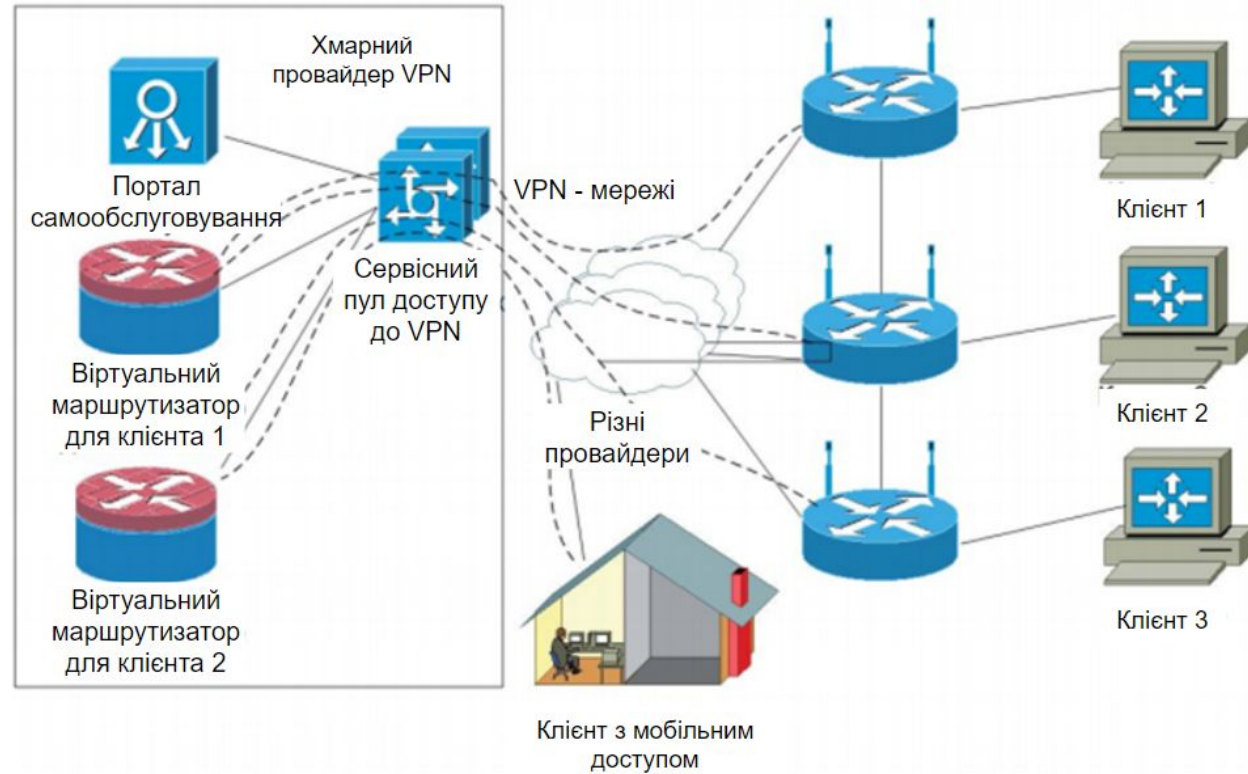


Демонстрація роботи VPN через проксі



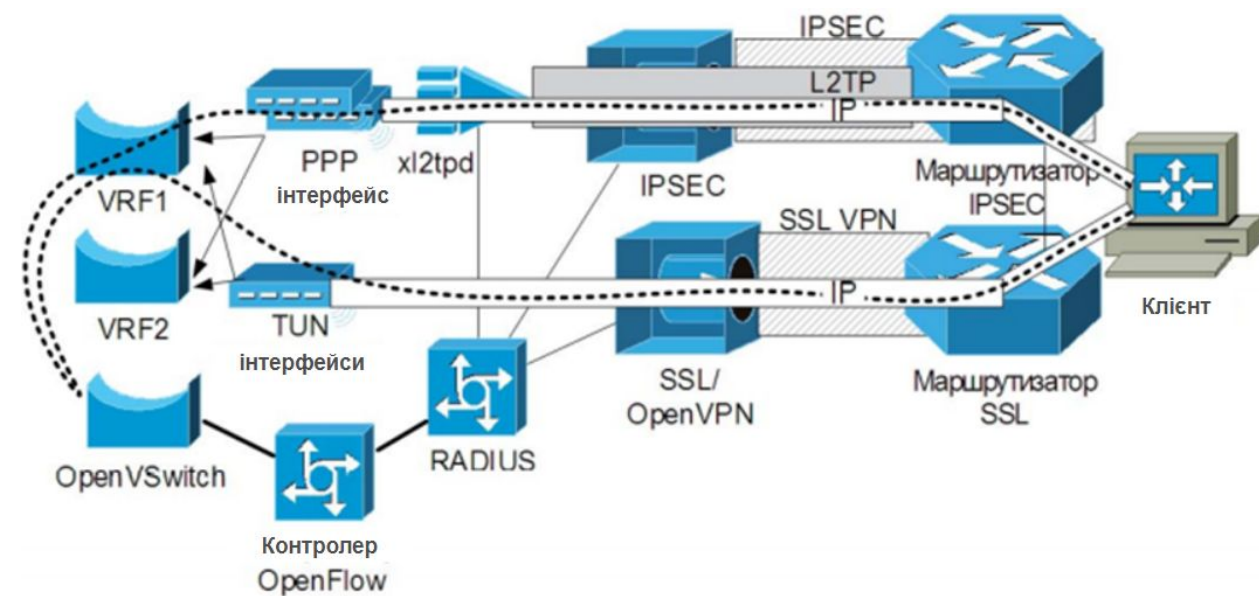
Демонстрація роботи трьох VPN одночасно

СТВОРЕННЯ МУЛЬТИСЕРВІСНОЇ VPN-МЕРЕЖІ З ДИНАМІЧНИМ АВТОНАЛАГОДЖЕННЯМ (1)

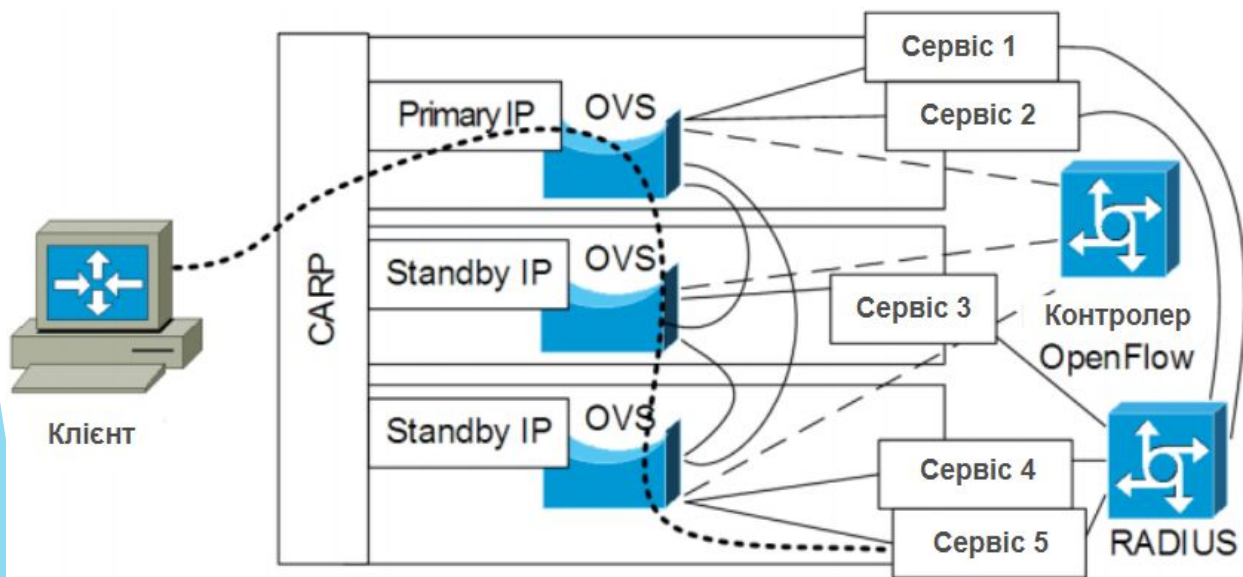


Хмарний провайдер VPN

СТВОРЕННЯ МУЛЬТИСЕРВІСНОЇ VPN-МЕРЕЖІ З ДИНАМІЧНИМ АВТОНАЛАГОДЖЕННЯМ (2)

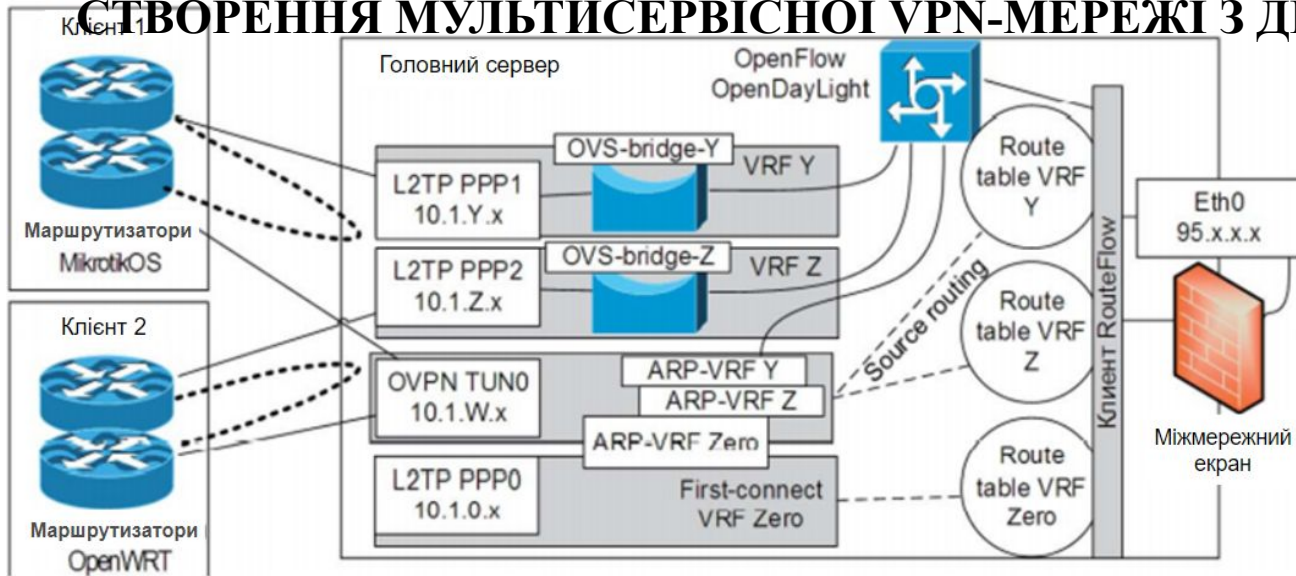


Одинарний VPN сервер з ізоляцією клієнтів

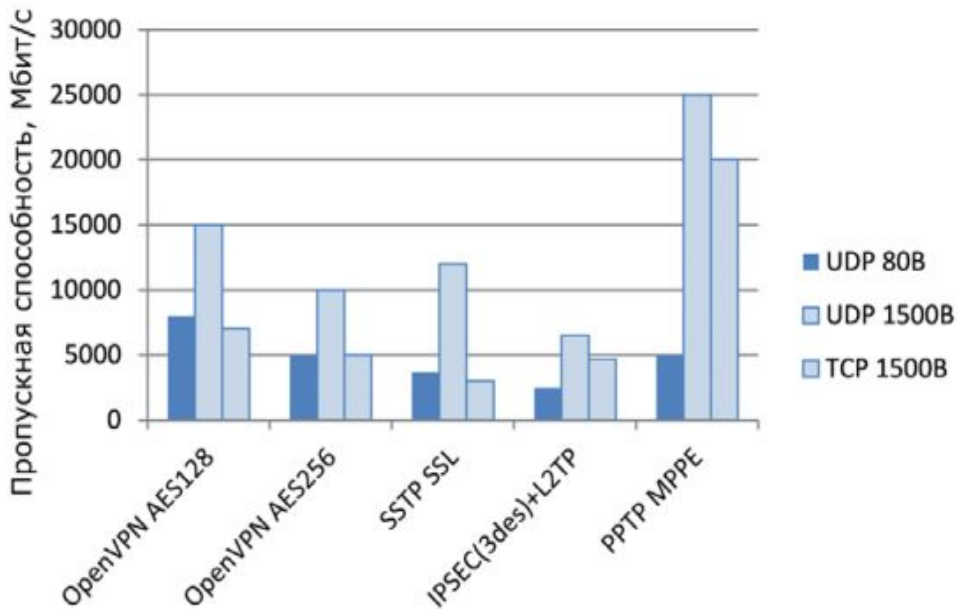


Балансування навантаження засобами OVS

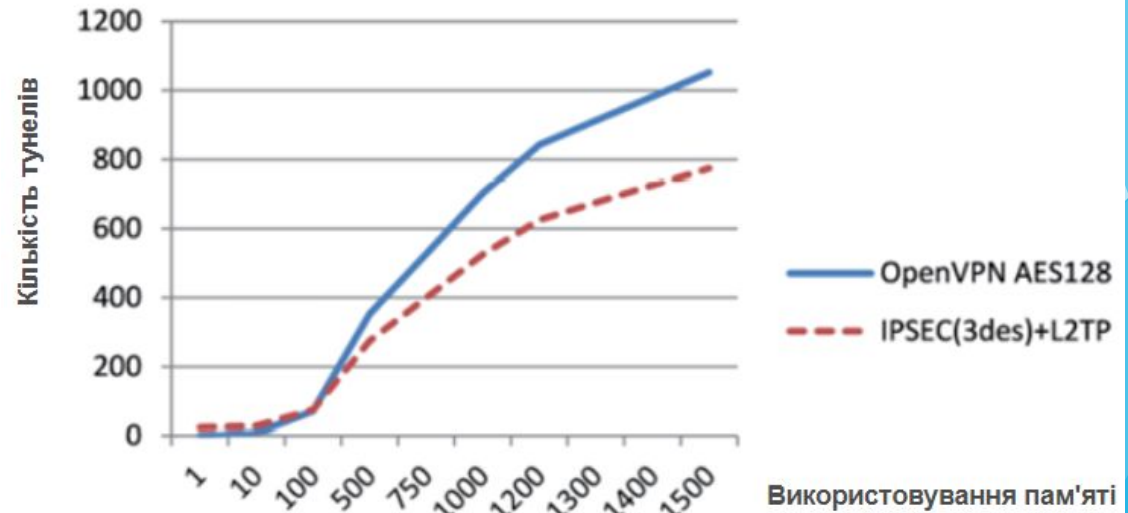
СТВОРЕННЯ МУЛЬТИСЕРВІСНОЇ VPN-МЕРЕЖІ З ДИНАМІЧНИМ АВТОНАЛАГОДЖЕННЯМ (3)



Експериментальний стенд NaaS VPN сервера

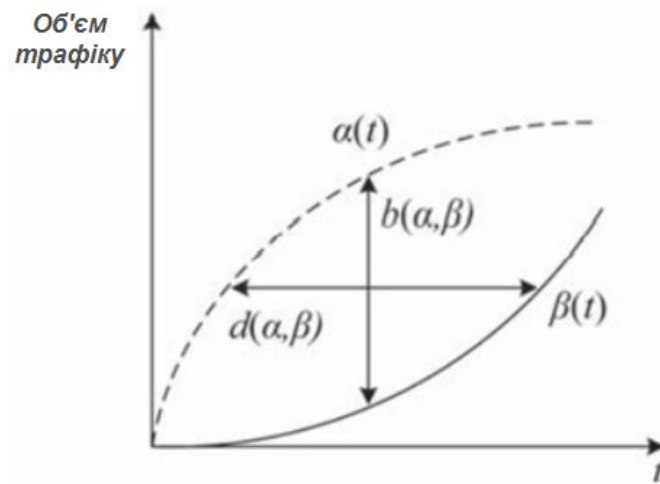


Оцінка продуктивності протоколів VPN



Оцінка використання пам'яті протоколів VPN

СТВОРЕННЯ МУЛЬТИСЕРВІСНОЇ VPN-МЕРЕЖІ З ДИНАМІЧНИМ АВТОНАЛАГОДЖЕННЯМ (4)



Функція обслуговування послідовної ланцюжка з n -вузлів $\beta(t)$ буде визначатися як $(\min, +)$ згортка функцій обслуговування окремих вузлів:

$$\beta(t) = \beta_1(t) \otimes \beta_2(t) \otimes \dots \otimes \beta_j(t) \otimes \dots \otimes \beta_n(t)$$

Базові криві (функції) теорії Network Calculus

ПОБУДОВА МАТЕМАТИЧНОЇ МОДЕЛІ РОЗРАХУНКУ КОМПЛЕКСНОЇ ОЦІНКИ РОБОТИ БАГАТОШАРОВОЇ ВІРТУАЛЬНОЇ МЕРЕЖІ

Для розрахунку питомої ваги групи критеріїв будемо використовувати нормуючі коефіцієнти. Розрахунок загального критерію захищеності VPN від загроз персональних даних $K_{пд}$ проводиться за формулою:

$$K_{пд} = K_{крипт} + K_{по} + K_{пр}$$

де $K_{крипт}$ – загальний критерій захищеності персональних даних від загроз, пов'язаних з недоліками в галузі забезпечення криптографічного захисту інформації; $K_{по}$ – загальний критерій захищеності персональних даних від загроз, зв'язаних з експлуатацією вразливостей стороннього ПО, $K_{пр}$ – загальний критерій захищеності від інших загроз персональних даних користувача.

Загальний критерій захищеності від виявлення використання користувачем засобів анонізації $K_{анон}$ та загальний критерій для користувача зручності $K_{пу}$ розраховуються як сума оцінок VPN за критеріями відповідної групи.

Після визначення ступеня відповідності VPN критеріям оцінки розраховується комплексний критерій оцінки VPN з урахуванням рівня захищеності.

$$K_{общ} = n_{довір}(a_{пд}K_{пд} + a_{анон}K_{анон} + a_{пу}K_{пу})$$

де $n_{довір}$ – коефіцієнт довіри розробнику, який приймає значення від 0 до 1; $a_{пд}$, $a_{анон}$, $a_{пу}$ – вагові коефіцієнти значущості першої, другої, третьої груп критеріїв відповідно.

ПРИКЛАД НАЛАШТУВАННЯ VPN МЕРЕЖІ З РОЗПОДІЛЕНИМИ ТОЧКАМИ ВХОДУ

Скрипт, що автоматизує процес розташування сертифікатів

```
#!/bin/sh

set -e

for domain in $RENEWED_DOMAINS; do
    case $domain in
        good.vpn)
            daemon_cert_root=/etc/ipsec.d/

            # Make sure the certificate and private key files are
            # never world readable, even just for an instant while
            # we're copying them into daemon_cert_root.
            umask 077

            cp "$RENEWED_LINEAGE/cert.pem" "$daemon_cert_root/certs/"
            cp "$RENEWED_LINEAGE/chain.pem" "$daemon_cert_root/cacerts/"
            cp "$RENEWED_LINEAGE/privkey.pem"
"$daemon_cert_root/private/"

            # Reread certificates
            /usr/sbin/ipsec reload
            /usr/sbin/ipsec purgecerts
            /usr/sbin/ipsec rereadall
            ;;
    esac
done
```

АПРОБАЦІЯ РЕЗУЛЬТАТІВ РОБОТИ

2021/59 - 8 червня 2021 р.

Міжнародна наукова інтернет-конференція "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення"(випуск 59)

Перелік секцій, авторів і тем їх доповідей

Відображається 60 елементів

Назва секції	Автор (автори)	Тема доповіді
Сортувати _	Сортувати _	Сортувати _
1. Інформаційні системи і технології	Амарій А.М., Мельничук С.В., Танаоск Ю.В.	Система відстеження перешкод та дорожніх знаків
1. Інформаційні системи і технології	Анненков І.О.	Формалізація поняття «інформація» стосовно агропромислового виробництва
1. Інформаційні системи і технології	Ареф'єв І.А., Черних О.П., Кучук Н.Г.	Створення універсальної системи збору та обробки даних з датчиків локального позиціонування
1. Інформаційні системи і технології	Бойчук І.І.	Отлад постачальників хмарних сервісів
1. Інформаційні системи і технології	Бондаренко А.С.	Розробка веб-журналу викладача
1. Інформаційні системи і технології	Братах Т.Ю.	Розробка програмного забезпечення для взаємодії з обладнанням лазерної гравірувальної установки через послідовний порт RS-232
1. Інформаційні системи і технології	Гриш А.І.	Розробка цифрового світлозвучного пристрою на базі мікропроцесорної плати Arduino
1. Інформаційні системи і технології	Давидова Г.Ю.	SMART-цілі. Ключовий чинник освітнього процесу
1. Інформаційні системи і технології	Дмитрик Т.В., Сторож Я.Б.	Використання інформаційних технологій у сфері навчання охорони праці
1. Інформаційні системи і технології	Завтур І.Ю.	Метод отримання зображень с веб-ресурсу шляхом парсингу
1. Інформаційні системи і технології	Зарудний Д.С.	Алгоритми обчислення основних характеристик для багатоканальних систем з повторними викликами
1. Інформаційні системи і технології	Зячук Я.І., Лазорів А.М.	Визначення узагальненого коефіцієнта технічного стану газоперекачувального агрегату на засадах нечіткої логіки
1. Інформаційні системи і технології	Кирилюк Я.О.	Розробка цифрового засобу реалізації MIDI-клавіатури на базі плати Arduino
1. Інформаційні системи і технології	Корбан Ю.В., Корбан Г.В.	Використання цільової функції для визначення впливу червоного кольору на емоційний стан особистості
1. Інформаційні системи і технології	Кропивницька В.Б., Кропивницький Д.Р.	Побудова діаграми Ісікави для структурного аналізу процесу буріння
1. Інформаційні системи і технології	Кулик Ю.А., Скоринович Б.В., Гавриляк В.Р.	Дослідження та аналіз інформаційної безпеки хмарних середовищ на прикладі AWS
1. Інформаційні системи і технології	Лапець О.В., Мала Ю.А., Рудовіч Є.А.	Забезпечення інформаційної безпеки в Україні
1. Інформаційні системи і технології	Лютак І.З., Хамурда А.В., Яцишин М.М.	Компонентний метод оптимізації веб-авторизації користувачів
1. Інформаційні системи і технології	Магас Д.М., Кропивницька В.Б.	Прогнозоване технічне обслуговування на основі штучного інтелекту в сфері видобутку нафти і газу
1. Інформаційні системи і технології	Мала Ю.А., Пирогов В.І., Лапець О.В.	Використання IT-технологій в навчальному процесі
1. Інформаційні системи і технології	Мартиненко К.В.	Хмарне середовище для розподіленої обробки даних
1. Інформаційні системи і технології	Мірошніченко А.В.	Побудова корпоративної комп'ютерної мережі з використанням технологій віртуалізації
1. Інформаційні системи і технології	Невчолода Л.В., Крикуненко К.М.	Застосування методів теорії масового обслуговування в управлінні ремонтом обладнання на машинобудівному підприємстві
1. Інформаційні системи і технології	Нікітюк О.О.	Термінальна комп'ютерна мережа на платформі оптоволоконної інфраструктури
1. Інформаційні системи і технології	Орловський В.О.	Автоматизована система розрахунків даних телекомунікаційної мережі
1. Інформаційні системи і технології	Пиріг М.М.	Розробка пристрою електроживлення з керуванням голосовими командами
1. Інформаційні системи і технології	Пікула Б.А.	Постановка та розробка методу розв'язання антагоністичної ігор з нечіткою матрицею типу2
1. Інформаційні системи і технології	Руденко І.В.	Модель розумного будинку на платформі одноплатного комп'ютера Raspberry Pi
1. Інформаційні системи і технології	Селєзньов А.О.	Розподілена комп'ютерна система контролю кліматичних показників на платформі Raspberry Pi
1. Інформаційні системи і технології	Соботник Е.Л., Бандура В.В.	Проблема надійності даних і її вирішення за допомогою технології GraphQL як засобу обміну інформацією між клієнтом та сервером у контексті WEB-застосувань
1. Інформаційні системи і технології	Сорока Д.О.	Комп'ютерна система ідентифікації змісту етикеток товарів за їх зображенням
1. Інформаційні системи і технології	Степанюк Л.О.	Веб-система для автоматизованої роботи з 3D-об'єктами
1. Інформаційні системи і технології	Яковенко К.О.	Багатошарова віртуальна мережа

ВИСНОВКИ

Віртуальні приватні мережі вже давно використовуються для забезпечення конфіденційності в Інтернеті. Вони гарантують такий рівень конфіденційності для комп'ютерів і користувачів Інтернету, який не може отримати в будь-якому іншому місці. Як це працює: програма створює цифровий тунель, через який трафік буде перенаправлений, захищаючи з'єднання від цікавих поглядів. Для цього з'єднання проводиться через віддалені сервери, маскуючи IP-адресу, часто з додаванням шифрування та інших функцій безпеки, що робить практично неможливим ідентифікувати користувача та мереду мережу і комп'ютер третім особам.

За результатами виконання атестаційної роботи було показано важливість використання багатопарових віртуальних комп'ютерних мереж при організації передачі даних в незахищених середовищах глобальної мережі Інтернет. Показано, що в даний час послуги віртуальної приватної мережі є досить гарячою темою, оскільки конфіденційність в Інтернеті піддається критиці з багатьох сторін. Компанії намагаються зібрати більше даних про своїх користувачів до такої міри, що вони стають надмірно нав'язливими, а країни розділилися в думках про те, як управляти ситуацією

В роботі запропоновано підхід до побудови віртуальних мереж зазначеного класу, створено такий прототип та проведено дослідження, які показують високий рівень ефективності використання таких мереж.

Мета роботи досягнута, атестаційна робота виконана у повному обсязі.

Дякую за увагу!