

Детектор Плагиата v. 2762 - Отчёт оригинальности: 20.01.2025 1:22:30

Проанализированный документ: Шила_mag_3_3.docx Лицензия: ВОЛОДИМИР МАТІЄВСЬКИЙ

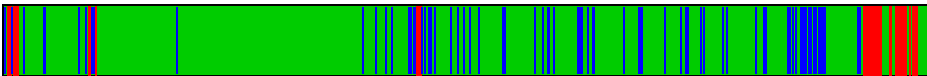
- Тип поиска: Поиск переписанного
- Язык: Uk
- Тип проверки: Интернет
- ТЕЕ и кодировка: DocX n/a

Детальный анализ тела документа:

Диаграмма соотношения частей:



Граф распределения зон:



Источники плагиата: 35

- 26% 1094 1. https://vstup.osvita.ua/r17/81/
- 13% 576 2. https://sci.ldubgd.edu.ua/jspui/bitstream/123456789/14259/1/Чорногуб_Придатко.pdf
- 8% 46 3. https://tecnobits.com/uk/як-налаштувати-protonvpn-для-підключення-до-певного-сервера-vpn/

Детали обработанных ресурсов: 177 - ОК / 16 - Ошибкак

Важные замечания:

Википедия:	Google Книги:	Сервисы платных работ:	Античит:
Обнаружена Wiki!	[не обнаружено]	[не обнаружено]	Обнаружено сокрытие!

Античит-отчет UACE:

1. Статус: АнализаторВключен Нормализатор Включен сходство символов установлено на 100%

2. Обнаруженный процент загрязнения UniCode: 11,2% с лимитом: 4%

3. Процент нераспознанных символов после нормализации: 6,5%

4. Все подозрительные символы будут отмечены фиолетовым цветом: Abcd...

5. Найдены невидимые символы: 0
- Рекомендации по оценке:
Особое внимание следует уделить анализу этого отчета! Предполагается, что этот документ содержит значительное количество символов, чуждых языку документа. Это прямое указание на то, что автор документа использовал специальное программное обеспечение\онлайн-веб-сервис, чтобы эффективно скрыть текст в попытке избежать обнаружения потенциального плагиата. Настоятельно рекомендуется передать это дело на более высокий уровень! В случае сомнений обращайтесь: в службу поддержки Детектора плагиата!
- Алфавитная статистика и анализ символов:

Активные ссылки (URL-адреса, извлеченные из документа):

URL не найдены

Исключённые ресурсы:


URL не найдены

Включённые ресурсы:

URL не найдены

Детальный анализ документа:

Міністерство освіти і науки України Державний заклад	
Цитирования: 0,1%	id: 1
«Луганський національний університет імені Тараса Шевченка»	
Навчально-науковий інститут математики та інформаційних технологій Кафедра	
Обнаружен Плагиат: 0,46% https://deps.snu.edu.ua/uk/fakultet-in... + 2 ресурсов!	id: 2
інформаційних технологій та систем Шила Максим Юрійович Аналіз програмного забезпечення для організації виконання лабораторних занять з обчислювальною технікою кваліфікаційна робота здобувача вищої освіти другого (магістерського) рівня освітньої програми	
Цитирования: 0,03%	id: 3
«Комп'ютерні мережі»	
Обнаружен Плагиат: 0,62% https://deps.snu.edu.ua/uk/fakultet-in... + 2 ресурсов!	id: 4
за спеціальністю 123 Комп'ютерна інженерія Особистий підпис _____ Максим ШИЛА Науковий керівник _____ Геннадій МОГИЛЬНИЙ, кандидат технічних наук, доцент кафедри інформаційних технологій та систем Завідувач кафедри _____ Микола СЕМЕНОВ, кандидат педагогічних наук, доцент кафедри інформаційних технологій та систем	
Полтава – 2025 АНОТАЦІЯ Шила Максим Юрійович. Тема: Аналіз програмного забезпечення для організації виконання лабораторних занять з обчислювальною технікою. Спеціальність: 123	
Цитирования: 0,03%	id: 5
«Комп'ютерна інженерія»	
Установа: ЛНУ імені Тараса Шевченка, 2025р. Магістерська робота містить: загальна кількість сторінок – 75, з них 68 – пояснювальна записка, 7 – додатки, 69 рисунків, перелік літератури – 18 джерел. Об'єкт дослідження – сучасні мережеві технології підтримки навчального процесу. Предмет дослідження – реалізація сучасних комп'ютерних технологій для організації лабораторних занять студентів в дистанційних умовах. Мета роботи – комплексний аналіз особливостей використання інформаційних ресурсів VMware Horizon, які створено на засадах програмного комплексу VMware та розробка додатку автоматизованого підключення до VPN. Результати роботи. В роботі проведено аналіз інформаційних ресурсів, наведено опис логічної та фізичної структури розташування цих ресурсів. Виділено основні типи. Для підвищення ефективності використання ресурсів наведено ґрунтовний опис процесів. Для автоматизації процесу розгортання VPN запропоновано використовувати спеціальний додаток CMAK –	
Цитирования: 0,1%	id: 6
« Connection Manager Administration Kit »	
(в українській версії	
Цитирования: 0,07%	id: 7
«Пакет адміністрування диспетчера підключень»	
). Досліджено особливості використання додатку CMAK. Висновок. На засадах CMAK розроблено додаток для автоматичного підключення до VPN типу L2PT комп'ютерів студентів з ОС WINDOWS. Ключові слова: навчальний процес, віддалений користувач, робочий стіл, віртуальні машини, клієнт, сервер, операційна система, vmware vsphere, vcenter, шлюз. ABSTRACT Shila Maksim Theme: Analysis of software for organizing laboratory classes with computer technology. Speciality: 123 "Computer Engineering" Institution: Luhansk Taras Shevchenko National University (LTSNU), 2025. The masters work contains: total number of pages – 75, of which 58 – explanatory note, 7 – enclosures, 69 - pictures, bibliography – 18 source. A research object is modern network technologies to support the educational process. The article of research is the implementation of modern computer technologies for organizing laboratory classes for students in remote conditions. An objective of the work is a comprehensive analysis of the features of using VMware Horizon information resources, which are created on the basis of the VMware software complex and the development of an application for automated connection to VPN. Job performances. Results of the work. The paper analyzes information resources, describes the logical and physical structure of the location of these resources. The main types are highlighted. To increase the efficiency of resource use, a thorough description of processes is provided. To automate the VPN deployment process, it is proposed to use a special CMAK application –	
Цитирования: 0,07%	id: 8
"Connection Manager Administration Kit".	
The features of using the CMAK application are investigated. Conclusions. Based on CMAK, an application has been developed for automatic connection to L2PT VPN of student computers with WINDOWS OS. Keywords. learning process, remote user, desktop, virtual machines, client, server, operating system, vmware vsphere, vcenter, gateway..	
Міністерство освіти і науки України	
Державний заклад	
Цитирования: 0,1%	id: 9
«Луганський національний університет імені Тараса Шевченка»	
Факультет (інститут)	
Обнаружен Плагиат: 0,41% https://vstup.osvita.ua/r17/81/ + 3 ресурсов!	id: 10
Інститут математики та інформаційних технологій (повна назва) Кафедра Інформаційних технологій та систем (повна назва) Галузь знань 12, Інформаційні технології (код, назва) Напрямок підготовки (спеціальність) 123	
Цитирования: 0,03%	id: 11
«Комп'ютерна інженерія»	

(код, назва) ЗАВДАННЯ на кваліфікаційну роботу освітньо-кваліфікаційного рівня	
» Цитування: 0,05%	id: 12
« магістр »	
(назва рівня) Студенту Шила Максим Юрійович (
 Обнаружен Плагиат: 0,29% https://sci.ldubgd.edu.ua/jspui/bitstre... + 2 ресурсов!	id: 13
(прізвище, ім'я, по батькові) Керівник кваліфікаційної роботи Могильний Геннадій Анатолійович (прізвище, ім'я, по батькові, науковий ступінь, вчене звання)	
<p>1. Тема роботи Аналіз програмного забезпечення для організації виконання лабораторних занять з обчислювальною технікою затверджена наказом по університету 2. Термін подання студентом закінченої роботи на кафедрі 3. Вихідні дані до роботи У результаті виконання роботи необхідно дослідити можливості програмного забезпечення для підключення до інформаційної системи IMIT; розробити рекомендації до різноманітних варіантів підключення, розробити додаток для автоматизації підключення до VPN; вбудовані системні можливості підтримки студентів (визначаються кількісні або (та) якісні показники, яким повинен відповідати об'єкт розробки) 4. Зміст пояснювальної записки (перелік питань, що їх належить розробити) Опис інсталювання клієнту vmware Horizon на ОС Windows та мобільний прилад Опис використання ВЕБ доступу, опис використання VPN, опис використання системних налаштувань ОС Windows та Horizon, використання CMAK (визначаються назви розділів або (та) перелік питань, які повинні увійти до тексту ПЗ) 5. Індивідуальний план виконання кваліфікаційної роботи № Заходи Термін виконання Вибір теми роботи, вивчення наукової літератури, затвердження теми та керівника. До 30 жовтня 2023 Аналіз літературних джерел за темою роботи. Розробка ТЗ. Розробка та апробація методики дослідно-експериментальної роботи. Подання структури теоретичної частини роботи (пояснювальної записки) та плану експериментальних досліджень. Другий тиждень жовтня 2024 Робота над теоретичною частиною. Подання теоретичної частини роботи для першого читання керівником. Розробка методики тестування До 1 грудня 2024 Усунення зауважень, урахування рекомендацій керівника. Аналіз структури програмного забезпечення. Перший тиждень грудня 2024 Поетапний аналіз та обговорення результатів. Перевірка стану виконання роботи. Перший тиждень грудня 2024 Урахування рекомендацій керівника, усунення недоліків, підготовка варіанта роботи до передзахисту. Оформлення документації до проекту. До 15 грудня 2024 Попередній захист роботи на кафедрі. За місяць до державної атестації Доопрацювання роботи з урахуванням рекомендацій після передзахисту. Розробка презентації. Підготовка графічних матеріалів. Перевірка на плагиат. Подання роботи науковому керівникові та рецензентові на підготовку відгуку та рецензії За 10 днів до державної атестації Подання на кафедру остаточного варіанта роботи, з відгуком керівника і рецензена. За 3 дні до державної атестації ЗМІСТ Перелік умовних позначень 7 Вступ 8 Розділ 1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА СИСТЕМИ 11 1.1 Аналіз варіантів використання 11 1.2 Загальна структура інформаційної системи 12 РОЗДІЛ 2. ЗАВАНТАЖЕННЯ КЛІЄНТІВ 20 2.1 Установка та завантаження клієнту 20 2.2 Приєднання до ресурсів за допомогою клієнта Horizon for mobile devices 27 Розділ 3. НАЛАШТУВАННЯ КЛІЄНТІВ 30 3.1 Налаштування клієнту WINDOWS 30 3.2. Налаштування та використання мобільного додатку 37 РОЗДІЛ 4 ВИКОРИСТАННЯ VPN З'ЄДНАННЯ 41 4.1 Автоматизація VPN за допомогою CMAK 41 4.2 Встановлення додаткового VPN з'єднання з внутрішніми інформаційними ресурсами НН IMIT 59 Висновки 65 Список літературних джерел 67 Додатки 69 Перелік умовних позначень ПК Програмний комплекс ОС Операційна система VDI? Що таке VDI? (Virtual desktop infrastructure) IDE Integrated Development Environment (Інтегроване середовище розробки) RDP Remote Desktop Protocol HTTP HyperText Transfer Protocol (Протокол передавання гіпертексту) CMAK Connection Manager Administration Kit AD Active Directory Esx 1 Elastic Sky X (Гіпервізор) MSN Microsoft Network IGMP Internet Group Management Protocol (Протокол керування групами Інтернету) IP Internet Protocol TCP Transmission Control Protocol (TCP, протокол керування передаванням) UDP (англ. User Datagram Protocol) — протокол польователських дейтаграм) НН IMIT Навчально-науковий інститут математики та інформаційних технологій ДЗ</p>	
» Цитування: 0,1%	id: 14
«Луганський національний університет імені Тараса Шевченка»	
<p>Вступ В період ковід пандемії, а потім під час відкритої збройної агресії російської федерації значна кількість підрозділів, підприємств, закладів освіти перешли на впровадженні дистанційних умов роботи. Кожен підрозділ вирішував це завдання враховуючи особливості своєї діяльності. Значна кількість навчальних закладів запровадила дистанційну та змішану форму навчання. Практично кожен навчальний заклад, викладацький склад почали впроваджувати різноманітні програмні засоби підтримки навчального процесу в дистанційних умовах. Було розпочато швидко впровадження програмного забезпечення засноване на сучасних інформаційно-комунікаційних технологіях. Викладачі були в поставлені в умови пошуку різноманітного програмного забезпечення. Вкрай активно стали впроваджувати програмні засоби для підтримки комунікацій зі студентами. До цих програм відносяться google meet, Skype та zoom. Доволі швидко було запроваджено методики викладання лекційних занять. Другим важливим аспектом підвищення ефективності навчального процесу стало запровадження програмних засобів спрямованих на підтримку самостійної роботи студентів. В цьому напрямку активно почали впроваджувати різноманітні LMS. Значна частина вищих навчальних закладів розпочала використовувати MOOBLE. Цей програмний засіб дозволяє не тільки організувати самостійну роботу студентів. Цю систему можна встановлювати на різні комп'ютери, навіть на домашні. Крім того, система mooble вирішило цілий комплекс питань з контролю процесу навчання, організації різних активностей для студентів, створення різноманітних видів завдань Таким чином в процесі переходу на дистанційну форму навчання вдалося вирішити цілі низьку питань. Всі ці заходи спрямовані на те що студенти використовують особисту обчислювальну техніку. Більш складна ситуація склалася в напрямку організації виконання лабораторних занять. В деяких випадках студент не в змозі виконати ці завдання на особистому комп'ютері. Особливо це стосується питань роботи зі складним програмним забезпеченням. Один із шляхів, вирішення даної проблеми є створення програмного комплексу, що надає студентам та викладачам можливість використовувати у віддаленому режимі різноманітне програмне забезпечення.</p>	

На даному етапі, рішення цієї проблеми всі рішення знаходяться на етапі впровадження, але існує ряд нових технологій, на основі яких можна впритул наблизитися до її вирішення. Тому в даній роботі можливо висловити наступне. Гіпотеза дослідження – використання спеціальних мережових технологій дозволить підвищити якість підготовки фахівців галузі ІТ-інформаційні технології Об'єкт дослідження – сучасні мережові технології підтримки навчального процесу. Предмет дослідження – реалізація сучасних комп'ютерних технологій для організації лабораторних занять студентів в дистанційних умовах. Мета роботи – комплексний аналіз особливостей використання інформаційних ресурсів [VMware Horizon](#), які створено на засадах програмного комплексу [VMware](#) та розробка додатку автоматизованого підключення до [VPN](#). Інноваційна новизна – знайдені особливості використання різних варіантів інформаційних ресурсів НН ІМІТ та розроблено автоматизованих програмний додаток для підключення до [VPN](#). Досягнення цієї мети передбачає вирішення таких основних завдань: Провести аналіз інформаційних ресурсів створених на засадах [VMware Horizon](#). Дослідити можливості використання клієнтських (студентських) приладів. Провести аналіз налаштування програмного забезпечення. Провести аналіз та розробку програмного забезпечення для автоматизації налаштування підключення до системи [VPN](#). У першому розділі проведено аналіз загальної структури інформаційних ресурсів. У другому розділі розглянуті типи та послідовність дій при інсталюванні додаткового програмного забезпечення для клієнтів = студентів. Третій розділ присвячений опису використання специфічних засобів для налаштування комп'ютерів студентів та налаштування необхідні використання мобільних приладів Четвертий розділ присвячений опису роботи програмного комплексу – [CMAK](#), на засадах якого розроблено додаток для автоматичного підключення до [VPN](#) типу [L2PT](#) комп'ютерів студентів з ОС [WINDOWS](#). Розділ 1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА СИСТЕМИ 1.1 Аналіз варіантів використання В НН ІМІТ Варіанти доступу: Клієнт [Vmware Horizon](#) – немає обмежень – рекомендується для постійної роботи – працює на всіх приладах – потребує завантаження та інсталювання клієнту [5]; Браузер (бажано Хром) – є обмеження на передавання / обмін файлами – рекомендується для ознайомлення – працює на всіх приладах – не потребує додаткового ПЗ; Додатковий [VPN](#) – тип [L2TP](#) – немає обмежень, повний доступ до всіх мережових приладів – розроблено спеціальний інсталятор для вирішення питань з маршрутизацією – надає повний доступ до всіх локальних ресурсів – рекомендуються для досвідчених користувачів для вирішення завдань по налаштуванню системи та створенню додаткових віртуальних машин – працює не на всіх приладах. Перелік адрес та інформація – існує дві системи, які об'єднані на рівні керування доступом та мають зв'язок з однією [AD](#). Ці системи повністю об'єднано та ліквідовано часткове дублювання ПЗ. На обох системах використовуються однакові імена користувачів та паролі. Зараз використовуємо: Для клієнту [Vmware Horizon](#) необхідно додати сервера: 176.105.199.98:4432 або [mitc.luguniv.edu.ua:4432](#) – основний Для браузера [https://176.105.199.98:4432](#) або [https://mitc.luguniv.edu.ua:4432](#) Для використання [VPN](#) Використання вбудованого у ОС [Windows](#) – не рекомендовано – весь трафік йде через канал НН ІМІТ (адреса сервера [VPN](#) 176.105.199.98) Спеціальний файл створений на засадах ПЗ [CMAK](#) [15] – входить до стандартного ПЗ [Windows Server](#) – розроблено та апробовано для ОС [Windows](#) 10 Рис.1.1 Загальний опис варіантів підключення 1.2 Загальна структура інформаційної системи Для створення умов виконання лабораторних робіт з використанням обчислювальної техніки в дистанційних умовах в НН ІМІТ розроблено нову локальну мережу (рис. 1.2) До складу локальної мережі входить: Пороговий роутер [Mikrotik](#) з ОС [ROUTE OS](#); Дві окремі мережі – 192.168.100.0/24 та 192.168.102.0/24 Спеціалізована мережа – не маршрутизуєма – 192.168.101.0/24 Два окремих сервера фірм [Supermikro](#) та [Dell](#). Загальний обсяг кластера складає: 96 ядер процесорів [Intel Xeon](#); понад 350 ГБ оперативної пам'яті; понад 60 000 ГБ дискового простору з 8 накопичувачів. Додатковий, внутрішній роутер з підтримкою [Wi-fi](#) – для об'єднання мережі [wi-fi](#) за допомогою спеціального [EAP](#) сервісу, який дозволяє інтегрувати імена користувачів та паролі Додатковий [wi-fi](#) роутер в режимі точки доступу Декілька керованих комутаторів Рис. 1.2 Загальна структура мережі НН ІМІТ Основні ресурси системи розташовано у мережі 192.168.100.0/24, до цієї мережі приєднано інші підрозділи університету, а комп'ютерні класи розташовано у основній мережі – 192.168.100.0/24. В цілому, основні інформаційні ресурси розташовано на двох сервках, на яких встановлено спеціальна ОС – гіпервізор – [VmWare ESXi](#) 7.0 [4]. Ця ОС пристосовано для створення основних завдань з віртуалізації. Для створення інтегрованого інформаційного середовища використовується цілий комплекс віртуальних машин, які керують корпоративним доступом до всіх віртуальних ресурсів (рис. 1.3). Рис.1.3 Загальна структура віртуальних серверів Ядро інформаційних ресурсів складають декілька віртуальних серверів, які приймають в кластері з двох фізичних серверів (хостів [esxi](#)) з адресами 192.168.100.12 та 192.168.100.22. На цих серверах налаштовано система [IDRAC](#) [2] та [IPMS](#) [1], налаштовані окремі мережові адаптери – 192.168.100.5 та 192.168.100.6 для керування [BIOS](#) та консоллю сервера (приклад роботи, дивись Додатки). Загальна схема підключення зображено на рис.1.4 Рис.1.4 Загальна схема підключення На одному з хостів (192.168.100.12) інстальовано [vmware vCenter](#) [3] – 192.168.100.24, який створює загальний кластер та керує всіма віртуальними машина всіх серверів (приклад роботи, дивись Додатки). На кожному сервері- хосту інстальовано віртуальна машина(приклад роботи, дивись Додатки): [Ms Windows Server](#) – 192.168.100.28 з додатковим компонентом [Ms AD](#) – контролер домену, та підтримка [DNS](#) [6,7], [Ms Windows Server](#) 192.168.100.8 з додатковим компонентом [Ms AD](#) – контролер домену, та підтримка [DNS](#). Додатково на сервері 192.168.100.28 налаштовано підтримку [UPS](#) (приклад роботи, дивись Додатки): сервер політики мережі для підтримки [Radius](#) клієнтів [6] (приклад роботи, дивись Додатки). В інформаційній системі ІМІТ використовуються 3 клієнти Пороговий роутер [Mikrotik](#) – м. Лубни для інтеграції доступу користувачів до [VPN](#) Внутрішній роутер для інтеграції доступу користувачів до [WIFI](#) Зовнішній роутер [Mikrotik](#) – м.Лубни для підтримки доступу до [SCORUS](#) Загальна схема розташування віртуальних серверів хосту 192.168.100.22 наведено на рис.1.5 Рис.1.5 Загальна схема віртуальних серверів хосту 1 На хості 192.168.100.22 інсталювано додатковий сервер [Ms Windows server](#) 192.168.100.11 з підтримкою файлових служб [9] та додано [Ms AD](#) для збереження інформації наступного типу (приклад роботи, дивись Додатки): Особистих файлів користувачів диск [K:](#) Даних профілю Загально доступних файлів – дисків [J:](#) [I:](#) Файлів переназначених тек користувачі –

» Цитування: 0,03%	id: 15
«Мої документи»,	
» Цитування: 0,02%	id: 16
«завантаження»	
» Цитування: 0,02%	id: 17
«Пошук»,	
» Цитування: 0,02%	id: 18
«Відео»	
та інше На хості 192.168.100.12 інстальовано додатковий сервер Ms Windows server з підтримкою vmware connection server (приклад роботи, дивись Додатки) та додано Ms AD для розгортання інших віртуальних машин для клієнтів vmware Horizon . Цей сервер додано до vmware Vcenter (приклад роботи, дивись Додатки). Загальна схема розташування віртуальних серверів хосту 192.168.100.12 наведено на рис.1.6. Рис.1.6 Загальна схема віртуальних серверів хосту 2 На хості 192.168.100.22 інстальовано додатковий сервер Ms Windows server з підтримкою RDP [10] та додано Ms AD для віддалено доступу клієнтів	
» Цитування: 0,05%	id: 19
«Віддаленого робочого столу»	
Цей сервер додано до vmware connection server На хості 192.168.100.22 інстальовано додатковий сервер Vmware UGA – шлюз для зовнішніх користувачів vmware Horizon . Цей сервер додано до vmware connection server Загальна структура віртуальних серверів Ms WINDOWS всіх хостів показано на рис.1.7 Рис.1.7 Загальна структура віртуальних серверів Ms WINDOWS Для підтримки об'єднаного середовища на сервері 192.168.100.28 - MS AD додано службу	
» Цитування: 0,05%	id: 20
«Сервер політики мережі»,	
яка дозволяє інтегрувати все інформаційне середовище. Загальна схема використання наведено на рис.1.8 Додатково для організації віддаленого доступу зовнішніх користувачів проведено налаштування всіх служб Vmware . За допомогою	
» Цитування: 0,05%	id: 21
«служби політики мережі»	
та основних можливостей VS AD налаштовано підключення всіх користувачів-студентів через вхідний пороговий роутер Mikrotik до основних інформаційних ресурсів. Загальний порядок проходження аутентифікації показано на рис. 1.9 Рис.1.8 Загальна структура інтеграції імен користувачів Рис.1.9 Загальна структура аутентифікації студентів РОЗДІЛ 2. ЗАВАНТАЖЕННЯ КЛІЄНТІВ 2.1 Установка та завантаження клієнту Запустіть браузер. Перейдіть на пошукову систему Google . У строчці пошуку наберіть download vmware horizon client (рис.2.1). Рис.2.1. Пошук у Google В результаті пошуку (рис.2.2) перейдіть за посиланням Download VMware Horizon Clients (сайту www.vmware.com) https://www.vmware.com/go/viewclients Рис.2.2. Результати пошуку З'явиться результат (рис.2.3). Рис.2.3 Сторінка вибору клієнта Увага! Для попередніх операційних систем Windows виберіть у лівій частині екрану	
» Цитування: 0,03%	id: 22
« Horizon 7 »	
(для Windows XP необхідно шукати та завантажувати клієнта версії 3.2 для Horizon 5) Оберіть	
» Цитування: 0,05%	id: 23
« GO TO DOWNLOADS »	
та перейдіть на наступну сторінку (рис.2.4). Рис.2.4. Завантаження клієнту Оберіть	
» Цитування: 0,03%	id: 24
« DOWNLOAD NOW »	
та збережіть файл. Після завантаження перейдіть до файлу клікніть правою кнопкою миші та оберіть	
» Цитування: 0,05%	id: 25
«Запустити від адміністратора»	
(рис.	
» Обнаружен Плагиат: 0,77% https://asiapac.medtronic.com/conte...	id: 26
2.5). Рис. 2.5 Початок установки клієнту Почнеться процес установки (рис.2.6). Рис.2.6. Установка клієнту Необхідно погодитись з перезавантаженням (рис.2.7) та перезавантажити комп'ютер . Рис. 2.7 Перезавантаження комп'ютеру Після перезавантаження оберіть іконку клієнту та запустіть програму (рис.2.8). Рис.2.	
8. Клієнт Horizon Оберіть	
» Цитування: 0,07%	id: 27
«+додати сервер /+ Add Server »	
(рис.2.9) та введіть IP адресу серверу (рис.2.10) та натисніть	
» Цитування: 0,02%	id: 28
« Connect ».	
Увала! IP адресу серверу надає викладач. Не розголошуйте цю адресу іншим особам. Рис.2.9 Додавання серверу Рис.2.10 IP адреса серверу Необхідно погодитись з сертифікатом та натиснути	
» Цитування: 0,02%	id: 29
« Continue »	

(рис.2.11). З'явиться вікно з привітанням (рис.2.12), у якому натисніть

» Цитування: 0,02%

id: 30

«Accept».

Рис. 2.11. Згода на під'єднання Рис. 2.12 Вітання інформаційної системи ННІФМІТ у відповідь з'явиться вікно з запрошенням до вводу імені користувача та паролю (рис.2.13). Ці данні необхідно взяти у викладача. Введіть та натисніть

» Цитування: 0,02%

id: 31

«Login».

Рис.2.13 Введення імені користувача та паролю З'явиться вікно з доступними вам ресурсами (рис.2.14). Двійним клацанням мишки завантажуйте необхідне програмне забезпечення. Рис. 2.14. Програмне забезпечення інформаційної системи ННІФМІТ 2.2 Приєднання до ресурсів за допомогою клієнта [Horizon for mobile devices](#) Запустіть [google play](#). Рис. 2.15 Зовнішній вигляд мобільного додатку У строчці пошуку наберіть [horizon client vmware](#). Рис.2.16 Використання [google play](#) Рис. 2.17 Завантаження та встановлення Почекайте завантаження та установить додаток. Знайдіть встановленого клієнта та завантажте клієнта Рис. 2.18 Зовнішній вигляд додатку Надайте всі відповідні дозволи Рис. 2.19 Створення необхідних дозволів Введіть адресу та опис з'єднання та натисніть

» Цитування: 0,02%

id: 32

«Connect»

Рис. 2.20 Додавання параметрів підключення Розділ 3. НАЛАШТУВАННЯ КЛІЄНТІВ 3.1 Налаштування клієнту [WINDOWS](#) ЗМІНА ПАРОЛЯ КОРИСТУВАЧА Для зміни пароля користувача виконайте наступні кроки: Увійдіть до відділеного робочого столу – подвійне клацання мишкою на відповідній піктограмі. В цей час, піктограма відділеного робочого столу має назву

» Цитування: 0,1%

id: 33

«(FMI)раб.стол(chry_2016)»,

однак вона може бути змінена, тому з'ясуйте у викладача. Якщо у системі декілька віддалених робочих столів – оберіть будь-який з них. Проведіть мишкою у верхню центральну частину екрану – з'явиться додаткове системне меню (рис. 3.1). Рис 3.1. Додаткове системне меню Оберіть

» Цитування: 0,02%

id: 34

«Ctrl+Alt+Del»

– з'явиться наступний перелік додаткового меню (рис.3.2). Рис. 3.2. Системне меню [Windows server](#) 2016. Оберіть пункт – Изменить пароль. Змініть пароль та обов'язково запам'ятайте його. Якщо ви забули пароль, то враховуйте, що адміністратор не може встановити пароль і не

» Цитування: 0,02%

id: 35

«бачить»

його. Адміністратор може призначити новий, інший пароль за вашим проханням. ЗМІНА МОВИ ВВОДУ В процесі роботи з програмних забезпеченням виникає необхідність змінити мову вводу з клавіатури (англійська, українська тощо). В цілому цей процес не відрізняється від вашого комп'ютеру з операційною системою [Windows](#). Слід врахувати, що в залежності від систем налаштувань, сполучення клавіш

» Цитування: 0,02%

id: 36

«Win+пробел»

може не працювати Рекомендується використовувати сполучення клавіш

» Цитування: 0,02%

id: 37

«Alt+Shift»

Примітка. Додаткові налаштування інших мов вводу виконується аналогічно комп'ютеру з операційною системою [Windows](#) (рис.3.3) Рис. 3.3 Налаштування мови вводу Використання інформаційних ресурсів власного пристрою В процесі роботи з інформаційними ресурсами ННІФМІТ надається можливість одночасного використання власних інформаційних ресурсів: накопичувачів, ВЕБ камери, [USB](#) накопичувачів тощо. Фактично виконується їх тимчасове поєднання, що надає можливість роботи в інтегрованому середовищі та дозволяє використовувати файли, принтери та флешки вашого комп'ютеру одночасно з файлами принтерами та програмним забезпеченням серверів. Системне програмне забезпечення поєднує (за вашою згодою) ваш комп'ютер з інформаційними серверними ресурсами. Це поєднання виконується тільки для вашого сеансу та тільки під час вашої роботи. Інші користувачі та адміністратори не мають доступ до ваших ресурсів. Всі ваші приєднанні ресурси будуть мати останні букви латинського алфавіту ([Z](#), [Y](#), [X](#); і так далі) Для цього необхідно після реєстрації у [Vmware Horizon Client](#) (рис. 3.4) натиснути піктограму налаштування Рис.3.4. Перехід до налаштувань [Vmware Horizon Client](#) Потім обрати у лівій частині

» Цитування: 0,07%

id: 38

«Drive & Folder Sharing»

Натиснути кнопку

» Цитування: 0,02%

id: 39

«Add»

та обрати теку або диск, який ви бажаєте тимчасово приєднати до серверної файлової системи (рис.3.5). На цьому рисунку обрано диск [C](#) : . Аналогічно виконайте додавання інших файлових ресурсів. Рис. 3.5 Поєднання власних файлових ресурсів (диск [C](#) :) Перелік загальних ресурсів інформаційної системи нніміт Перелік та призначення різноманітних дисків інформаційної системи має свої особливості в залежності від ресурсу до якого ви приєдналася: окремий додаток, окрема віртуальна машина, віддалений робочий стіл. Однак, на цей час, ряд ресурсів є незмінними в незалежності від виду приєднання: це диски [J](#) : [K](#) : та [M](#) :. Наприклад, на рис. 3.6 відображено стан дисків у віддаленому робочому

столи Рис. 3.6. Перелік дисків В цей час використовуються наступні мережеві диски: **H:** (**prog**) – службовий, додаткові програмні засоби – тільки читання; **I:** (**buffer**) – загальний, для тимчасового зберігання повний доступ – всі мають право видалити та створити інформацію; **J:** (**inst**) – інсталяції програмних засобів, для використання на особистих комп'ютерах – тільки читання; **K:** (Ваше ім'я) – особистий диск користувача – доступне тільки певному користувачу; **L:** (Ваше ім'я) – особистий диск користувача – доступне тільки певному користувачу; Останні літери алфавіту (**Z:**, **Y:**, **X:**,.....) – тимчасово підключені певні ресурси особистого комп'ютера користувача, для об'єднання з особистим комп'ютером – доступ тільки користувача. Завершення роботи з віддаленим робочим столом Для завершення роботи натисніть кнопку

Цитирования: 0,02%

id: 40

«Win»

, потім значок вимкнути, а потім – відключитися (рис 3.7, 3.8). Рис 3.7. Завершення роботи Рис 3.8. Завершення роботи Тому пропонується розглянути і провести експеримент архітектуру з виділенням сервером. Дана архітектура володіє більш низькою надійністю, але можливо дозволить поліпшити якість переданих звукових (відео) повідомлень. 3.2. Налаштування та використання мобільного додатку Може виникнути помилка. Треба налаштувати. Натисніть

Цитирования: 0,02%

id: 41

«Cancel»

та поверніться до головного екрану та натисніть значок налаштування. Рис. 3.9 Помилка при першому завантаженні Оберіть

Цитирования: 0,03%

id: 42

«Security option»,

а потім

Цитирования: 0,03%

id: 43

«Security mode»,

Рис. 3.10 Налаштування безпеки Оберіть режим

Цитирования: 0,05%

id: 44

«Ні перевіряти сертифікат»

натисніть

Цитирования: 0,02%

id: 45

«OK».

Поверніться до головного екрану додатку та знову спробуйте приєднатися Рис. 3.11 Обирання режиму перевірки сертифікату Повинно з'явиться повідомлення – привітання. Натисніть

Цитирования: 0,02%

id: 46

«Accept».

Введіть ім'я користувача та пароль, а потім натисніть

Цитирования: 0,02%

id: 47

«Done»

Рис. 3.12 Реєстрація у системі Ви увійшли до системи. Повинно відобразитись вікно з різноманітними додатками 1 – завантажити віддалений робочий стіл 2 – від'єднатися та вийти із системи 3 – налаштування 2 3 1 Рис.3.14 Режими роботи віддаленого робочого столу 1 – розгорнути екран 2 – інші програми 3 – різноманітні налаштування 3 2 1 Рис. 3.15 Зовнішній вигляд робочого столу **Windows** РОЗДІЛ 4 ВИКОРИСТАННЯ **VPN** З'ЄДНАННЯ 4.1 Автоматизація **VPN** за допомогою **СМАК** В інтернеті мало інструкцій з автоматизації підключень користувачів (студентів) до **VPN** Один з варіантів - використання спеціального пакету **СМАК**, тому в рамках даної роботи розроблено інструктивну послідовність дій щодо використання цього пакету Рис.4.1 Зовнішній вигляд підключення Отже, у ПН ІМІТ, використовується варіант підключення до **VPN**. Це вимагає створення спеціальних інструкцій для студентів та викладачів щодо створення підключень до нашого **VPN** сервера для користувачів **Windows**. Для розробки програми для підключення, надаючи користувачеві готову програму, що створює підключення з наперед визначеними нами параметрами і готове до роботи в умовах нашої мережі. Здійснити це нам допоможе вбудований у **Windows Server** компонент -

Цитирования: 0,1%

id: 48

« Connection Manager Administration Kit »

(в українській версії

Цитирования: 0,07%

id: 49

«Пакет адміністрування диспетчера підключень»

). Отже, для того, щоб встановити **СМАК**, необхідно запустити

Цитирования: 0,03%

id: 50

«Диспетчер сервера»

і встановити новий компонент

Цитирования: 0,07%

id: 51

«Пакет адміністрування диспетчера підключень».

Весь поточний приклад базується на **Windows Server** 2016, російська версія. Встановлення компонента у диспетчері сервера: Рис 4.2. Додавання компонентів серверу Після інсталяції пакет адміністрування доступний з меню

Цитирования: 0,02%

id: 52

«Пуск»

або аплет

»

Цитування: 0,02% «Адміністрування»	id: 53
на панелі керування. Після запуску CMAK нас вітає майстер пакета адміністрування. Рис. 4.3 Завантаження CMAK Натискаємо	
Цитування: 0,02% «далі».	id: 54
У наступному вікні майстер пропонує вибрати сімейство операційних систем, для яких створюємо підключення. Під Windows Server це " Windows 7 , Vista	
Цитування: 0,02% ", або "	id: 55
Windows Server 2003, Windows XP та Windows 2000». Втім, якщо виберемо пункт з Windows 7 і Vista , підключення підійде і для Windows 8. Рис 4.4 Вибір ОС Після вибору операційних систем необхідно створити новий профіль, або відредагувати існуючий, якщо він є (вперше створюється новий). Рис 4.5 Вибір профілю Далі потрібно ввести ім'я створюваного підключення (так з'єднання буде відображатися в мережевих підключеннях Windows) і ім'я файлу, який буде запускати користувач. Ім'я файлу не повинно перевищувати вісім символів та мати розширення. Рис 4.6 Вибір служби Після назви підключення – майстер дасть можливість додати ім'я сфери. Оскільки використовувати провайдера як шлюз аутентифікації на VPN сервері планується, то цей пункт пропускається. Рис 4.7 Вибір сфери На наступному етапі ми пропонуємо додати дані з телефонної книги інших існуючих профілів, щоб не вводити їх по новій. Т.к. інших створених профілів ми не маємо — йдемо далі. Рис 4.8 Об'єднання профілів Далі нам необхідно вказати IP -адресу VPN сервера для підключення. Рис 4.9 Призначення серверу Є можливість вказати єдину постійну адресу (у мережі IMIT – 176.105.199.98), або текстовий файл, що містить набір адрес для підключення, які будуть надані користувачеві на вибір. Файл має наступний формат: [Settings] default = UpdateURL = Message = Де, default =ім'я VPN сервера, який буде використовуватися за замовчуванням (якесь із наведених нижче, наприклад	
Цитування: 0,07% « My VPN Server1 »	id: 56
); UpdateURL =Посилання на текстовий файл зі списком сервером (щоразу при підключенні цей файл буде оновлюватися з вказаної URL); Message = Повідомлення для користувача, наприклад, будь ласка, виберіть сервер для підключення. [VPN Servers] My VPN Server1 = my1.example.com My VPN Server2 = my2.example.com My VPN Server3 = my3.example.com У мережі IMIT обмежимося єдиним сервером. На цій же сторінці можемо відзначити пункт використовувати ті самі облікові дані для аутентифікації як на VPN -сервері, так і на dial-up з'єднанні (якщо хочемо його використовувати перед створенням VPN -підключення). Наступне вікно дозволяє перейти до налаштувань тунелю. Рис 4.10 налаштування тунелю Натиснувши	
Цитування: 0,02% «змінити»,	id: 57
можна налаштувати основні параметри VPN -з'єднання. На вкладці	
Цитування: 0,02% «загальні»	id: 58
можна вибрати типи протоколів, які використовуються в мережі	
Цитування: 0,02% « IPv4 »,	id: 59
Цитування: 0,02% « IPv6 »,	id: 60
або те й інше, а також вимкнути	
Цитування: 0,1% «загальний доступ до файлів та принтерів»,	id: 61
якщо він не потрібний. Рис 4.11 Налаштування з'єднання Вкладка IPv4 дозволяє встановити параметри для протоколу IPv4 . Серед налаштувань: DNS , WINS , використання підключення як шлюз за замовчуванням та стиснення. У деяких інструкціях, у випадку, якщо нам потрібно було не використовувати з'єднання VPN як шлюз за промовчанням - пропонувалося залишити тут цю настройку включеною, а потім використовувати у файлі зі статичними маршрутами директиву REMOVE_GATEWAY . Досвідченим шляхом встановлено, що ця інструкція працює не коректно і призводить до помилки, коли хост після підключення взагалі перестає використовувати свій шлюз за замовчуванням. І це налаштування ця відпрацювала цілком коректно, тобто. якщо не потрібно використовувати VPN - сервер як шлюз за промовчанням, то просто знімаємо тут цю галочку і додаємо пізніше статичні маршрути для мереж, в які потрібно ходити через VPN . Рис 4.12 Налаштування з'єднання IPv4 Майже такі ж налаштування для протоколу IPv6 . У мережі IMIT – не використовуємо Рис 4.13 Налаштування з'єднання IPv6 На вкладці	
Цитування: 0,02% «Безпека»	id: 62
можна вибрати потрібний нам тунельний протокол (PPTP , L2TP , SSTP), причому можемо вибрати єдиний, а можемо вибрати черговість спроб підключення. Наприклад, якщо виберемо спочатку використовувати L2TP , після L2TP буде використовуватися PPTP , та був SSTP тощо. Також доступні різні параметри шифрування. Для L2TP , наприклад, можна вказати розділений ключ. У такому разі після налаштування VPN з'єднання майстер запропонує зашифрувати наш ключ PIN -кодом, який доведеться ввести користувачеві під час встановлення з'єднання. У цьому вікні можна налаштувати методи аутентифікації — більш безпечний у випадку EAP , чи MS-CHAP 2 , наприклад. Для цієї статті було обрано пріоритет L2TP із розділеним ключем. Рис 4.14 Налаштування безпеки На вкладці	
Цитування: 0,02% «Безпека»	id: 63

«додатково»	
можна вказати DNS -суфікс , який буде використовуватися клієнтським з'єднанням. Вікно для введення розділеного ключа та PIN -коду для його шифрування. Рис 4.15 Налаштування безпеки та ключів Далі майстер пропонує ввести телефонну книгу для додзвону до dial-up сервера. У мережі ПН IMIT це не актуально, тому знімаємо галку з пункту	
Цитування: 0,08%	id: 64
«автоматично завантажувати оновлення телефонної книги»	
та натискаємо	
Цитування: 0,02%	id: 65
«далі».	
Рис 4.16 Налаштування телефонної книги Так як, dial-up для нас не актуальний, то і наступне вікно пропускаємо так само. Рис 4.17 Налаштування додаткових записів Далі нам пропонується зробити оновлення для таблиці маршрутизації. Якщо це актуально, додаємо файл маршрутів. Наведу приклад файлу маршруту. Допустимо, якщо необхідно , щоб клієнт ходив у мережу 192.168.100.0/24 через VPN підключення (VPN -мережа має відмінну адресацію від мережі 192.168.98.0/24), при цьому шлюз за умовчанням має залишитися свій. Тоді необхідно додати текстовий файл за маршрутом наступного змісту:	
Цитування: 0,28%	id: 66
« ADD 192.168.0.0 MASK 255.255.255.0 default METRIC default IF default ».	
З'ясовано, що файл повинен бути обов'язково у кодуванні ANSI , а не UTF-8 , наприклад. Якщо прибрали галочку з пункту	
Цитування: 0,1%	id: 67
"Зробити це підключення основним шлюзом клієнта",	
ніяких директив REMOVE_GATEWAY тут писати не потрібно. Рис 4.18 Додавання маршрутів Можна також вказати URL -адресу на файл, що містить таблицю маршрутизації, вона оновлюватиметься при кожному підключенні. У наступному вікні майстра можна вказати параметри проксі-сервера для Internet Explorer під час підключення VPN . Можливі наступні варіанти - взагалі не налаштовувати параметри проксі (перший пункт), використовувати вже налаштовані користувачем параметри (другий пункт), або використовувати попередньо налаштований файл, який містить параметри проксі (третій варіант). У мережі IMIT не використовується проксі-сервер, тому залишаємо цей пункт без зміни Рис 4.19 Додавання проксі У наступному вікні можна налаштувати додаткові дії. Наприклад, нам може знадобитися запуск будь-якої програми або скрипта при кожному запуску підключення. У такому разі натискаємо	
Цитування: 0,02%	id: 68
«створити»	
та переходимо до налаштувань. Рис 4.20 Додавання дій Тут, крім нашої програми або скрипту, можна вибрати різні події, при настанні яких буде виконано дію. Наприклад, після підключення або при помилці. Якщо відзначити пункт	
Цитування: 0,15%	id: 69
«включити в цей профіль служби вказану програму дії користувача»,	
то програма буде скопійована в профіль підключення (корисно на випадок, якщо запускаємо щось нестандартне, чого на інших комп'ютерах немає). Якщо передбачається взаємодія програми з користувачем, то цьому етапі слід зазначити відповідну галочку. Рис 4.21 Додавання дій певної спрямованості Далі можна визначити малюнок, відмінний від малюнка, що відображається у підключенні за замовчуванням . І також для телефонної книги: Рис 4.22 Додавання малюнку Можна змінити іконку підключення: Рис 4.23 Додавання малюнку На наступному екрані можна встановити свій hlp -файл довідки, або залишити довідкову інформацію, запропоновану за промовчанням . Рис 4.24 Додавання допомоги Далі можна вказати інформацію про технічну підтримку (наприклад, телефони цілодобової служби тощо). Рис 4.25 Додавання підтримки Додати інформацію ліцензійної угоди. Загалом, якщо потрібно підтвердження згоди користувача на будь-що - задати це теж можна, вибравши текстовий файл. Рис 4.26 Додавання ліцензійних умов Якщо потрібно включити в наш профіль, що створюється додаткові файли (наприклад, вони можуть використовуватися програмою, або скриптом, який могли вибрати вище) - то слід їх вибрати на наступному екрані. Рис 4.27 Додавання додаткових файлів На цьому налаштування закінчено і залишається натиснути	
Цитування: 0,02%	id: 70
«далі»	
у наступному вікні та	
Цитування: 0,02%	id: 71
«готово»	
у фінальному – побачимо шлях, яким створився профіль для підключення. Рис 4.27 Завершення Перед тим, як копіювати цей профіль клієнту, варто згадати про ще один момент: якщо залишити все як є, то у випадку з PPTP — підключення пропонуватиме вказати регіональні налаштування телефону, що зовсім не потрібно. Справа виправляється редагуванням файлу з розширенням cms , який лежить у профілі створеного підключення. Отже, необхідно в цьому файлі, у секції	
Цитування: 0,07%	id: 72
"[Connection Manager]"	
додати параметр	
Цитування: 0,05%	id: 73
« connectbtype =1»	
і зберегти файл. Робити це слід після створення підключення, тому що після завершення	

створення або правки профілю — файли перезаписуються і параметр з великою ймовірністю загубиться. Для поширення серед студентів та викладачів папку з профілем потрібно копіювати та встановлювати підключення у два кліки. Запускаємо **exe**-файл з ім'ям підключення: Рис 4.28 Розгортання Після ствердної відповіді з'явиться вікно, де можна вибрати - встановлюється підключення тільки для даного користувача, або для всіх, а також вказати створити ярлик підключення на робочому столі. Рис 4.29 Розгортання для користувачів Студентові залишиться лише ввести дані для підключення та, можливо, підтвердити механізму **UAC** своє бажання надати системні привілеї нашому підключенню (у разі, якщо потрібно внести маршрут, або запустити програму, яка потребує системних привілеїв). 4.2 Встановлення додаткового **VPN** з'єднання з внутрішніми інформаційними ресурсами НН ІМІТ 1. Запустити файл для інсталяції (з правами адміністратора). Клацніть правою кнопкою миші та оберіть

» Цитування: **0,07%** id: **74**

«Запуск от имени администратора»

(див. рис. 4.30) Рис.4.30 Запуск с правами адміністратора Зараз назва файлу -

ifmit_1_j2tp.exe. Назва може змінюватись 2. З'явиться повідомлення- погодьтесь , натисніть

» Цитування: **0,02%** id: **75**

«ДА».

Потім з'явиться ще одне повідомлення рис 4.31 – Натисніть

» Цитування: **0,02%** id: **76**

«ДА».

Увага, можуть бути певні особливості, в залежності від налаштувань системи Рис.4.31.

Запит дозволу на встановлення 3. У відповідь – з'явиться повідомлення про ПІН код

(рис.4.32). Введіть 1234 . Натисніть

» Цитування: **0,02%** id: **77**

«OK».

Увага, ПІН-код може змінюватись. Рис.4.32. Введення ПІН коду 4. З'явиться наступне

повідомлення (рис.4.33). Оберіть бажані параметри, (наприклад, як на рис.4.33) та

натисніть

» Цитування: **0,02%** id: **78**

«OK»

Рис. 4.33. Умови інсталяції 5. Програма заважиться – з'явиться повідомлення – рис. 4.34.

Введіть ваше ім'я користувача – у полі

» Цитування: **0,02%** id: **79**

«Пользователь»,

ваш пароль – у полі

» Цитування: **0,02%** id: **80**

«Пароль»,

ваш домен (Взяти у викладача) в полі

» Цитування: **0,02%** id: **81**

«Домен»

та натисніть

» Цитування: **0,02%** id: **82**

«Подключить»

Рис.4.34. Реєстрація В результаті: а) на робочому столі з'явиться ярлик – рис.4.35. Рис.4.35.

Ярлик на робочому столі б) в нижній лівій частині екрану при натисканні на значку

» Цитування: **0,02%** id: **83**

«мережа»

повинно з'явитися з'єднання з назвою

» Цитування: **0,07%** id: **84**

« 2tp for net IFMIT»,

дивись рис 4.36. Рис.4.36. **VPN** з'єднання Для використання цього з'єднання необхідно 1 В

лівій нижній частині екрану натиснути на значок мережа» та обрати з'єднання з назвою

» Цитування: **0,07%** id: **85**

« 2tp for net IFMIT»,

дивись рис 4.36. 2. З'явиться вікно

» Цитування: **0,03%** id: **86**

«Параметри **VPN**»

(рис.4.37). Знову оберіть

» Цитування: **0,07%** id: **87**

« 2tp for net IFMIT»

та натисніть Рис. 4.37. Вибір з'єднання 3. З'явиться наступне (рис.4.38) – оберіть

» Цитування: **0,02%** id: **88**

«Подключиться»

Рис.4.38. Підключення 3. З'явиться вікно реєстрації (див. рис.4.34) – ваше ім'я користувача

– у полі

» Цитування: **0,02%** id: **89**

«Пользователь»,

ваш пароль – у полі

» Цитування: **0,02%** id: **90**

«Пароль»,

ваш домен (Взяти у викладача) в полі

» Цитування: 0,02%

id: 91

«Домен»

та натисніть

» Цитування: 0,02%

id: 92

«Подключить».

4. З'явиться вікно додавання маршрутів – рис.4.39. Натисніть

» Цитування: 0,02%

id: 93

«Продолжить»

Рис. 4.39 Додавання маршрутів Після роботи у ваших мережевих з'єднаннях (значок мережі у лівому нижньому куті екрану повинно бути повідомлення про підключення. Рис.11. Успішне приєднання. Висновки В процесі переходу на дистанційну та змішану форму навчання вдалося вирішити цілі низьку питань. Однак, більш складна ситуація склалася в напрямку організації виконання лабораторних занять. В деяких випадках студент не в змозі виконати ці завдання на особистому комп'ютері. Особливо це стосується питань роботи зі складним програмним забезпеченням. В межах запропонованої магістерської роботи проведено комплексний аналіз особливостей використання інформаційних ресурсів ННІМІТ та шляхи впровадження інформаційних ресурсів, які дозволяють підвищити якість підготовки фахівців галузі ІТ-інформаційні технології Таким чином, знайдені особливості використання різних варіантів підключення до інформаційних ресурсів ННІМІТ. В роботі проведено аналіз інформаційних ресурсів, наведено опис логічної та фізичної структури розташування цих ресурсів. На засадах ґрунтовного аналізу виділено основні типи Система віртуальних серверів [Ms Windows](#). Система служб [VMware vsphere](#) та [Horison](#). Система підтримки засобів аутентифікації. Для підвищення ефективності використання ресурсів наведено ґрунтовний опис процесів Інсталювання клієнтів. Налаштування клієнтів. Оскільки використання вбудованого у ОС [Windows](#) приводе до того, що весь трафік йде через канал ННІМІТ. Запропоновано розробити спеціальний додаток для налаштування [VPN](#) з'єднання студентів. Для автоматизації процесу розгортання [VPN](#) запропоновано використовувати спеціальний додаток [CMAK](#) –

» Цитування: 0,1%

id: 94

« [Connection Manager Administration Kit](#) »

(в українській версії

» Цитування: 0,07%

id: 95

«Пакет адміністрування диспетчера підключень»

). Досліджено особливості використання додатку [CMAK](#). На засадах [CMAK](#) розроблено додаток для автоматичного підключення до [VPN](#) типу [L2PT](#) комп'ютерів студентів з ОС [WINDOWS](#) Список літературних джерел [IPMI](#) [

Обнаружен Плагиат: 1,47% <https://sci.l dubgd.edu.ua/jspui/bitstre...> + 2 рецензов!

id: 96

Електроний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Intelligent_Platform_Management_Interface_IDAC [Електроний ресурс]. – Режим доступу: <https://www.deli.com/en-in/ip/dl/open-manage-idrac-vcenter> [Електроний ресурс]. – Режим доступу: <https://www.vmware.com/products/cloud-infrastructure/vcenter-esxi> [Електроний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/VMware_ESXi_horison [Електроний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/VMware_ESXi [Обзор доменных служб Active Directory](#) [Електроний ресурс]. – Режим доступу: <https://learn.microsoft.com/ru-ru/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-active-directory> [Електроний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Active_Directory [Сервер политики сети \(NPS\)](#) [Електроний ресурс]. – Режим доступу: <https://learn.microsoft.com/ru-ru/windows-server/networking/technologies/nps/nps-top> [Настройка роли сервера файловых служб](#) [Електроний ресурс]. – Режим доступу: <https://learn.microsoft.com/ru-ru/windows-server/networking/branchcache/deploy/configure-the-file-server-what-is-a-file-server> [Що таке сервер віддалених робочих столів?](#) [Електроний ресурс]. – Режим доступу: <https://serversolutions.com.ua/blogs/news/%D1%89%D0%BE-%>

Обнаружен Плагиат: 0,02% <https://tecnobits.com/uk/як-налашту...> + 12 рецензов!

id: 97

[%D1%82%D0%B4%D0%B5%D1%80%D0%B2%D0%B5%D1%80-%D0%B2%D1%96%D0%B4%D0%B4%D0%B0%D0%BB%D0%B5%D0%BD%D0%B8%D1%85-%D1%80%D0%BE%D0%B1%D0%BE%D1%87%D0%8%D1%85-%D1%81%D1%82%D0%BF%D0%BB%D1%96%D0%B2?](#)

[srsltid=AfmBOoqLDIIFkmHENKLrGf2PMxLios3PGddXu4An6bql6qM992pHlq](#) Вибір мережевої технології [

Обнаружен Плагиат: 1,03% <https://sci.l dubgd.edu.ua/jspui/bitstre...> + 3 рецензов!

id: 98


Електроний ресурс]. – Режим доступу: <https://studfile.net/preview/9906498/page:3/> [ПРОТОКОЛИ TCP / IP I UDP](#). [МЕРЕЖИ TCP / IP](#) [Електроний ресурс]. – Режим доступу: https://stud.com.ua/84321/ekonomika/protokoli_merezhi [Мережа та мережева технологія](#). [Мережні інформаційні технології](#) [Електроний ресурс]. – Режим доступу: <http://ni-news.pp.ua/tehnika-tehnologiy/2369-merezha-ta-merezhnaya-tehnologiya-merezhn-nformatsiya/> [Windows, Linux, macOS: порівняння та особливості](#) [Електроний ресурс]. – Режим доступу: <https://www.globallogic.com/ua/insights/blogs/basics-of-operating-systems/> [Мережні технології](#) [Електроний ресурс]. – Режим доступу: <https://uk.wikipedia.org/wiki/%D0%9C%>

Обнаружен Плагиат: 0,02% <https://tecnobits.com/uk/як-налашту...> + 5 рецензов!

id: 99

[%D0%B5%D1%80%D0%B5%D0%B6%D0%BD%D1%96_%D1%82%D0%B5%D1%85%D0%BD%D0%](#)

[Difference between Unicast, Broadcast and Multicast in Computer Network](#) [

 Обнаружен Плагиат: **0,54%** <https://sci.ldubgd.edu.ua/jspui/bitstre...> + 2 ресурсов! id: **100**

Електронний ресурс]. – Режим доступу:
<https://www.geeksforgeeks.org/difference-between-unicast-broadcast-and-multicast-in-computer-network/>
[Wikipedia - the free encyclopedia](#) [Електронний ресурс]. – Режим доступу:
https://en.wikipedia.org/wiki/Application_layer - [Application layer](#) Стек протоколів [TCP/IP](#)
[Електронний ресурс]. – Режим доступу: <http://www.znanius.com/3608.html> Додатки Рис. 1. Зовнішній вигляд [Vmware esxi](#) 7 Рис. 2. Зовнішній вигляд [IDRAC](#) Рис. 3. Зовнішній вигляд [Vmware Vcenter](#) Рис. 4. Зовнішній вигляд [UPS](#) Рис. 5. Вхід до [Vmware connect server](#) Рис. 6. [Vmware connect server](#) Рис. 7. [Vmware connect server](#) – [application end desktop](#) Рис. 8. Перелік серверів [Ms Winwows](#) Рис. 9. Служба [DNS end AD user](#)

Заявление об ограничении ответственности:

Этот отчет должен быть правильно истолкован и проанализирован квалифицированным специалистом, который несет ответственность за оценку!

Любая информация, представленная в этом отчете, не является окончательной и подлежит ручному просмотру и анализу. Пожалуйста, следуйте инструкциям: [Рекомендации по оценке](#)

Детектор Плагиата - Ваше право на оригинальность! © SkyLine LLC