КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (4), 2019
ISSN 2663 - 4023

DOI 10.28925/2663-4023.2019.4.2431
УДК 004.7

Абрамов Вадим Олексійович
кандидат технічних наук, доцент,
доцент кафедри кафедри комп’ютерних наук і математики,
Київський університет імені Бориса Грінченка, Київ, Україна.
OrcID:0000-0002-8026-1475
v.abramov@kubg.edu.ua

ЗАСТОСУВАННЯ КОМБІНОВАНИХ МОДЕЛЕЙ КОМПЮТЕРНИХ МЕРЕЖ В НАВЧАЛЬНОМУ ПРОЦЕСІ

Анотація. Здійснюється огляд засобів моделювання комп’ютерних мереж з метою створення методики вивчення відповідних дисциплін у ЗВО (закладі вищої освіти). Здійснений аналіз позитивних та негативних властивостей віртуальних та фізичних засобів моделювання комп’ютерних мереж. Зроблено висновок, що найкращими для навчальних закладів є комбіновані моделі, які є досить бюджетними і дозволяють складати і вивчати практично необмежені топології мереж, а також отримати досвід роботи з реальним фізичним обладнанням. Аналіз засобів віртуального моделювання показує, що в них закладені засоби взаємодії віртуальної мережі з зовнішнім реальним обладнанням. Це дає можливість створити комбіновану платформу, у якій частина моделі є віртуальна а частина реально фізична. Це дозволяє бюджетними засобами швидко створювати моделі великої кількісті мереж і дає змогу студентам отримати досвід роботи з апаратними засобами в умовах наближеним до реальних промислових мереж. Платформу комбінованого моделювання дуже зручно використовувати для дослідження систем з «Інтернету речей». Вона допомагає під час проектування моделювати і дослідити реальні системи керування великою кількості віртуальних «Розумних речей», які представлені в новому симуляторі Cisco Packet Tracer 7.0. Цими віртуальними речами можна керувати з зовнішніх засобів реального світу через ноутбуки, планшети і т.і. Створювати для цього реальні програми керування і відповідні програмні засоби і налаштовувати їх в умовах максимального наближення до реальності. Нові технології моделювання є підґрунтям для виникнення нових методика навчання, які використовуються у Київському університеті імені Б. Грінченка.

Ключові слова: комп’ютерні мережі, віртуальні моделі, реальне обладнання, інтернет речей; системи керування; вбудовані системи; дистанційні лабораторії; методика викладання.

1. ВСТУП

Процес навчання, як відомо, безпосередньо пов'язаний з експериментами, зі створенням і усуненням критичних і аварійних ситуацій. При цьому вивчати можна спостерігаючи роботу реальних об'єктів, але це дуже тривалий і дорогий шлях. У навчальному процесі частіше вибирають альтернативне навчання на моделях.

Навчальне моделювання дозволяє визначати оптимальні топології, адекватний вибір мережевого обладнання, робочі характеристики мережі та можливі етапи майбутнього розвитку. При цьому на моделі можна випробувати різні режими роботи мережі, наприклад, вплив шторму широкомовних запитів або випробувати режим колапсу (для Ethernet), що неможливо застосувати в працюючої мережі.

При вивченні комп'ютерних мереж використовують, як віртуальні, так і фізичні моделі, побудовані на реальному обладнанні. Тип моделі істотно впливає на її вартість, що важливо для навчальних закладів.

Постановка проблеми. Застосування симуляторів, особливо безкоштовних, безумовно зменшує вартість навчальної моделі, але наявні недоліки знижують цей ефект. Для віртуального моделювання мережі потрібні значні ресурси, особливо оперативна пам'ять. Крім того, швидкість розгортання реальних пристроїв набагато більше ніж віртуальних, іноді це має значення. Тому частину мережі зручно і доцільно створювати на основі реального обладнання.

Незважаючи на високу вартість реального обладнання, відмовлятися від фізичних моделей не бажано. Студентам цікавіше і більше подобається працювати з реальним обладнанням, вони отримують значно більше враження від роботи з реальними комутаторами, маршрутизаторами, лініями зв'язку, структурованими кабельними системами, а значить ефект навчання вище. Працюючи з реальним обладнанням, студенти стають більш впевненими в своїх силах. Крім того, не всі функції реальних пристроїв можна змоделювати на симуляторі. Наприклад, найпростіше - створення СКС.

Аналіз останніх досліджень і публікацій. Існує досить велика кількість симуляторів і емуляторів для віртуального моделювання обладнання Cisco Systems та інших виробників.

Найбільш відомими і поширеними прикладами є навчальні курси академії Cisco. У них використовується симулятор Cisco Packet Tracer, який дозволяє моделювати основні функції обладнання Cisco. Крім того, в цих курсах деякі лабораторні роботи виконуються на фізичних моделях мереж. Для цього навчальні заклади закуповують досить дороге реальне мережеве обладнання.

Симулятор Cisco Packet Tracer доступний як під Windows, так і для Linux, безкоштовно для учнів Мережевий Академії Cisco. Його особливість це дружність і логічність інтерфейсу. У ньому зручно перевіряти роботу сервісів DHCP / DNS / HTTP / SMTP / POP3 / NTP. Зручно в режимі simulation побачити переміщення пакетів з уповільненням часу. Однак він обмежений у своїх можливостях і моделює тільки обладнання Cisco [1,2,3].

Відомі й інші програми. Для моделювання мережевих топології широко використовується контейнер віртуальних машин GNS3. Він являє собою графічний інтерфейс для емулятора Qemu и Dynamips. Емулятор Dynamips працює зі справжніми прошивками IOS. До GNS3 можна підключати віртуальні машини VirtualBox або VMware Workstation і створювати досить складні схеми, при бажанні можна піти далі і випустити його в реальну мережу. Платформа GNS3 (www.gns3.com) широко використовується як в ході навчання, так і для проектування і супроводу реальних мереж. Вона забезпечує серйозне вивчення предмета і орієнтована на повністю вільні рішення [4, 5]. Для роботи емулятор GNS3 вимагає значних витрат ресурсів комп'ютера і також має певні обмеження по функціям.

Ще один симулятор Boson NetSim працює тільки під Windows і виконує лабораторні роботи Cisco. Є ще такі програми як Cisco CSR (вартість ліцензії на 1 рік близько 1000 $), Cisco IOU (офіційно не поширюється). eNSP - симулятор обладнання Huawei подібний Cisco Packet Tracer, є демонстраційна версія.

Різних типів моделей багато але жодний не є найкращим для навчального процесу.

Мета статті. Підвищення ефективності вивчення і формування професійної компетентності при вивченні базових технологій комп'ютерних мереж і дисциплін, пов'язаних з ними на ґрунті використання моделювання комп’ютерних мереж при мінімальних витратах ресурсів і обладнання.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Аналізуючи позитивні та негативні властивості усіх типів моделей, виникає бажання взяти позитив з кожного. Тому найкраще рішення для навчального процесу використовувати моделі мереж з комбінацією віртуальних і реальних компонентів. Найбільш популярні програми дозволяють випускати віртуальне обладнання в реальну мережу. Як Packet Tracer, так і GNS3 дозволяють підключати віртуальну мережу до реальної. Так виникає комбінована модель на основі фізичних і віртуальних засобів. Найбільш дорогим обладнанням є маршрутизатори (router), їх доцільно закупити в мінімальній кількості, а все інше моделювати віртуально на сімуляторі.

Такий підхід дозволяє проводити експерименти на реальних працюючих мережах з використанням їхніх ресурсів, підключаючи до них віртуальні мережі. Також дозволяє одночасно працювати декільком користувачам. Кожен робить свою віртуальну мережу і включає її в реальну. Так можна збирати дуже великі складні мережі. Реальна і все віртуальні мережі працюють як одне ціле і дозволяють проводити експерименти в кожної віртуальної підмережі.

Пакет GNS3 складається з набору окремих самостійних програм, склад яких можна змінювати в ході інсталяції. Окремі додатки відповідають за власні блоки функцій. Наприклад, для імітації віртуальних маршрутизаторів використовується Dynamips, емуляції комп'ютерів-хостів - VirtualBox і т. д. GNS3 грає роль платформи, що дозволяє зручно ув’язати їх в цілісне наочне середовище. Доступні всілякі плагіни, розширення та інші корисні опції. Свіжі версії необхідних компонентів завантажуються з мережі автоматично в ході установки пакета GNS3.

Оригінальна особливість GNS3 - можливість перекинути місток від віртуальності до реальності. Наприклад, в базу пакета входять додатки Wireshark і WinPcap, що дозволяють маніпулювати даними, переданими в реальних мережах. З'являється дуже цікава можливість роботи не тільки в локальному віртуальному середовищі, а й у реальному, можна поєднати в одній моделі віртуальні та фізичні пристрої.

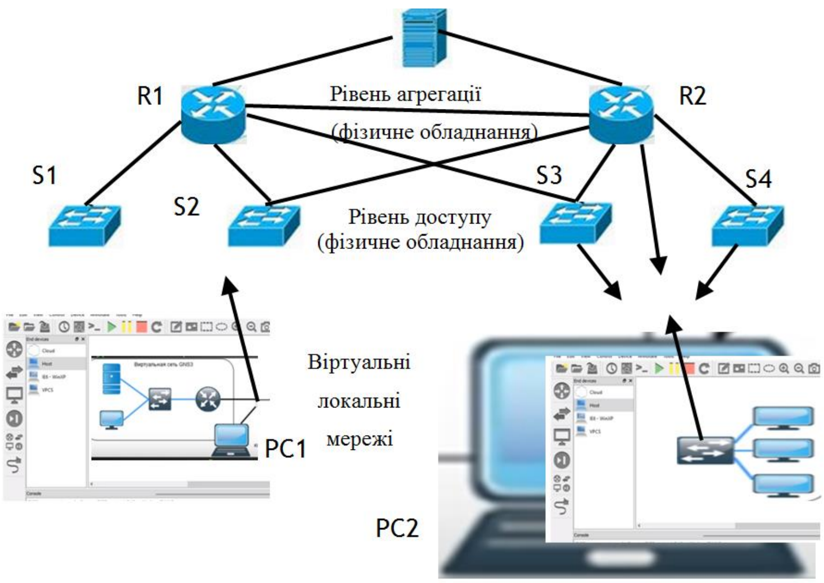

Рис. 1. Приклад комбінованої моделі мережі на ґрунті GNS3 і фізичного обладнання.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (4), 2019
ISSN 2663 - 4023

GNS3 підтримує дві віртуальні машини: Dynamips і Qemu. Вибір саме цих машин для включення в GNS3 обумовлений наявністю в їх складі розвинених засобів для з'єднання між собою операційних систем. Віртуальна машина Qemu в складі GNS3 під управлінням Ubuntu виявилася найкращим вибором для організації віртуальної лабораторії.

Віртуальна машина Dynamips дозволяє запустити всередині себе реальну IOS для дуже широкого класу пристроїв Cisco. Однак при роботі з Dynamips слід підбирати параметри для зменшення навантаження на центральний процесор. Без належних налаштувань Dynamips використовує всі ресурси комп'ютера вже для топології з трьох маршрутизаторів.

Для створення комбінованої моделі на грунті GNS3 будемо використовувати метод підключення віртуальної мережі до реальної фізичної за допомогою логічного інтерфейсу (віртуального адаптера) loopback [5].

На рис.1 зображено приклад комбінованої моделі мережі на ґрунті GNS3 і фізичного обладнання. Модель має реальну частину, що складається з реального фізичного обладнання, яке забезпечує функції агрегації і доступу для локальних комп’ютерів PC1, PC2 та інших. На цих комп’ютерах розгорнуто платформу GNS3, створено віртуальні мережі, які через мережевий інтерфейс відповідного комп’ютера мають доступ до реальної мережі.

Комбінована модель дозволяє досить бюджетними засобами створювати велику кількість різних мереж і водночас працювати з реальним фізичним обладнанням. При необхідності подальшого зменшення коштовності мережі використовується організація програмного роутінга з допомогою звичайних комп’ютерів з кількома мережевими картами. [6].

Комбінована модель дуже зручно підходить також до моделювання рішень в області інтернету речей. Інтернет речей - це концепція мережі, яка складається з пристроїв, які здійснюють обмін даними між фізичним світом и комп'ютерними системами, з допомогою використання стандартних протоколів зв'язку. Інтернет речей (IoT) - це не просто розумний будинок або розумне підприємство, експерти прогнозують що найближчим часом мільярди пристроїв будуть вирішувати найрізноманітніші завдання в різних областях. Так вони вже вирішують безліч завдань. На рис. 2 зображено типову функціональну схему роботи розумного пристрою з хмарою Azure, яку пропонує CISCO.

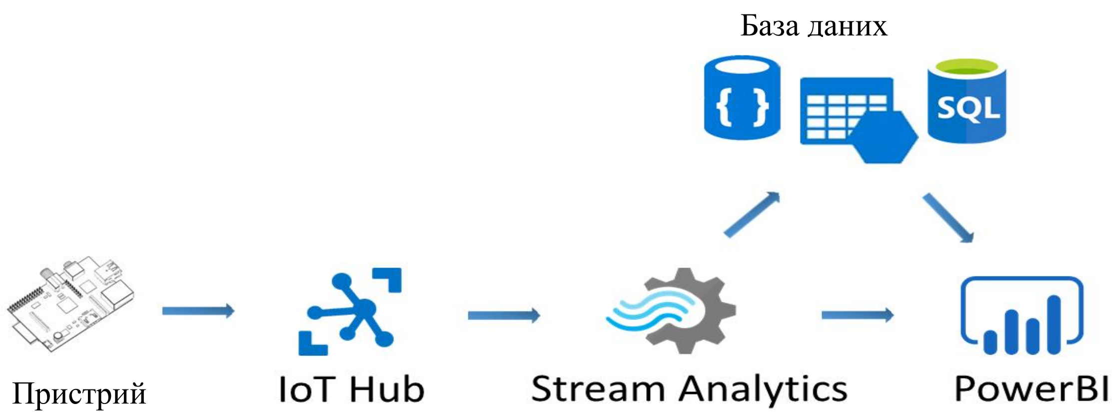

Рис.2. Основні сервіси Azure для Інтернету речей

На схемі пристрій взаємодіє з IoT хабом. IoT хаб це Центр інтернету речей. Він може як отримувати дані з пристроїв, так і відправляти їм повідомлення і команди [7].

Крім цього, взаємодіяти з пристроями можуть і інші сервіси, наприклад, Event Hub. Найбільша відмінність в цих сервісах в тому, що IoT Hub може працювати з мільйонами пристроїв, в той час як Event Hub працює з тисячами пристроїв, володіє дуже високою пропускною здатністю і може отримувати мільйони повідомлень в секунду. Друга істотна відмінність в тому, що IoT хаб може відправити команду на пристрій, в той час як Event хаб не може. В цілому у IoT хаба можливостей більше. Найчастіше Event хаби використовуються в проектах не для взаємодії з пристроями, а в якості проміжних сервісів [8].

Починаючи з 7 версії програми Cisco Packet Tracer у програмі з'явилась підтримка Internet of Things (Інтеренет речей). Серед кінцевих пристроїв є домашній шлюз для управління речами з Інтернету. Є велика кількість компонентів розумного дому: розумний кондиціонер, розумна кавоварка, батарея (акумулятор), блютуз динамік, детектори карбону діо- та моно-оксиду, розумний вентилятор на стелі, розумні двері, розумний нагрівач, розумні двері гаражу, розумна лампа, детектор руху, і т.і. Інші розумні речі розташовано на вкладках Розумне місто, Індустріальне, Енергосистема, Виконавчі механізми, Сенсори.

Таким чином розумних пристроїв дуже багато, мати таку кількість фізичного обладнання для моделювання не можливо и тому треба використовувати їх у вигляді віртуальних моделей. Але об'єднувати їх у мережі і керувати доцільно через реальну мережу. Наприклад, керування всім цим віртуальним господарством може здійснюватися через реальний смартфон [9].

Інтернет речей використовується в компаніях для виконання профілактичного обслуговування, відстеження продуктивності виробничих ліній, моніторингу пристроїв, віддаленого виявлення і усунення неполадок - у всіх областях, які мають величезний вплив на розмір одержуваного прибутку. За оцінкою компанії McKinsey Інтернет речей здатний забезпечити отримання прибутку в 2,3 трильйона доларів США у всьому світі до 2025 р

Це - одна з причин значного зростання використання Інтернету речей. Таке зростання супроводжується проблемами управління і забезпечення безпеки. У міру того як компанії все більше покладаються на Інтернет речей у своїй діяльності, спостерігається все більша потреба у відповідній безпечної IoT-платформі для збору і аналізу всіх цих даних, а також для управління ними.

Центр Інтернету речей Azure - це повністю керована служба, яка забезпечує надійний і захищений двонаправлений обмін даними між мільйонами пристроїв і серверної частиною рішення.

Центр Інтернету речей Azure забезпечує безпечний зв'язок завдяки використанню унікальних облікових даних безпеки пристрою і контролю доступу; кілька варіантів глобальної взаємодії між пристроями і хмарою; сховище, що містить відомості про стан кожного пристрою і його метадані; просте підключення пристроїв, так як використовуються бібліотеки пристроїв для більшості популярних мов і платформ.

Центр Інтернету речей Azure є хмарний шлюз, що з'єднує пристрої Інтернету речей і збирає дані для автоматизації та активації бізнес-аналітики. Можливості двонаправленого обміну даними означають, що при отриманні даних з пристроїв ви також можете відправляти команди і політики назад на пристрої, наприклад для поновлення властивостей або виклику дій управління пристроєм.

Інтелектуальні пристрої стикаються з різними загрозами безпеці, починаючи фізичним втручанням і закінчуючи зломом IP-адреси. Спеціально для цього і

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (4), 2019
ISSN 2663 - 4023

розроблена служба IoT Edge, яка охоплює різні профілі ризиків і сценарії розгортання, а також забезпечує належний захист, очікувану від всіх служб Azure [10].

Практично необмежені можливості у створенні різних конфігурацій мереж дозволяють створювати цикл лабораторних робіт за принципом усунення одного недоліку [11]. Тобто студенти в черговий лабораторної роботі вивчають переваги і недоліки відповідної мережі і пропонують шляхи усунення одного найважливішого, на їхню думку, недоліку. У наступних лабораторних роботах їм пропонується як цей недолік усунуто в реальних працюючих мережах і т.д. Наприклад, методи ліквідації колізій або широкомовних штормів. Загальна структура комбінованої моделі інтернету речей зображено на рис. 3.

Збільшення кількості підключених пристроїв і обсягу даних збільшує потребу в безпеці цих даних. Чим більше мережа, тим більше децентралізованою вона стає. Це дозволяє використовувати більшу кількість точок доступу в мережі, що призводить до більшої кількості вразливостей. Значна кількість пристроїв, які обмінюються даними через IoE, передаватимуть дані з небезпечних місць, але ці передачі повинні бути безпечними. Однак забезпечення вирішення IoE може бути ускладнено через велику кількість датчиків, смарт-об'єктів і пристроїв, підключених до мережі. Потенційна шкода, яка викликана доступом незахищених пристроїв до мережі організації, є серйозною проблемою для фахівців з безпеки.

При моделюванні мережі на комбінованій платформі можуть бути розглянуті питання безпеки, запобігання загрозам. Фахівці з мережевої безпеки моделюють і намагаються запобігти майбутнім атаки, зводячи до мінімуму наслідки успішних атак.

В архітектурі безпеки, використовуються пристрої для контролю доступу, перевірки вмісту і застосування політик: Міжмережеві екрани, Системи запобігання вторгнень (IPS). Рішення безпеки Cisco Application Centric Infrastructure (ACI) захищають середовище, повністю інтегруючи індивідуальні технології безпеки для потреб конкретного додатка. Це рішення забезпечує цілісний, заснований на політиці підхід до безпеки, який знижує вартість і складність.

Найважливішою частиною політики безпеки є навчання користувачів [12]. Люди, керовані політикою безпеки, повинні не просто знати про цю політику; вони повинні розуміти і дотримуватися цього, щоб забезпечити безпеку людей, даних і речей.

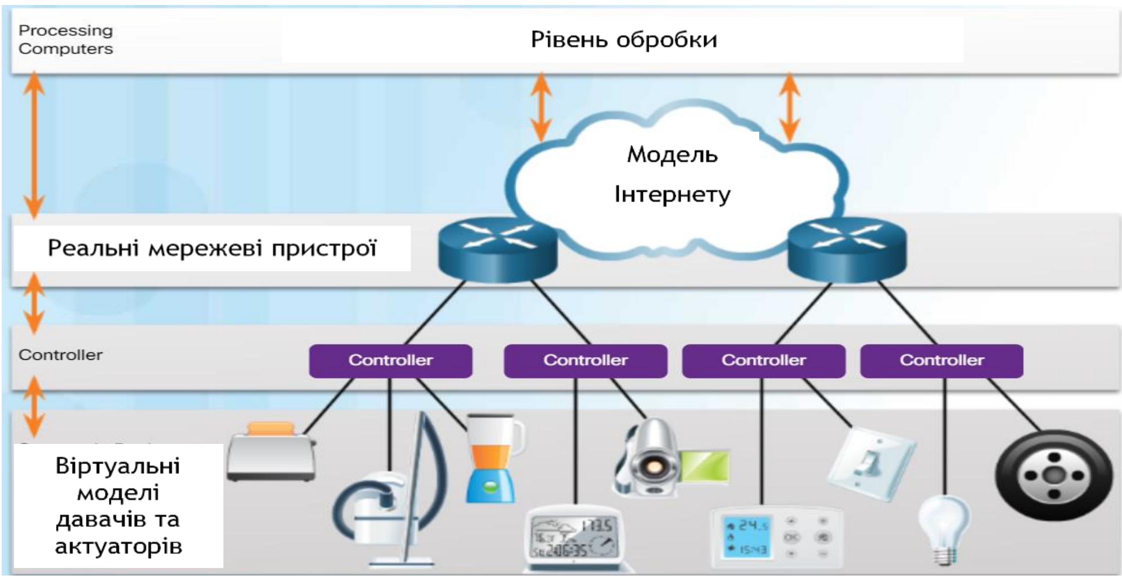

Рис. 3. Комбінована модель інтернету речей.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

1. Комбінована платформа має суттєві переваги і перспективи використання і розвитку. Нові сучасні технології моделювання мереж є підґрунтям для виникнення нових методика навчання, які використовуються у Київському університеті імені Б. Грінченка.
2. Можливість моделювати досить складні комп'ютерні мережі обумовлена широким діапазоном змін базової фізичної платформи і практично необмеженими можливостями моделювання віртуальних мереж.
3. Число одночасно працюючих студентів обмежується тільки числом портів комутаторів базової платформи. Студенти мають можливість набути досвіду роботи як з реальним мережевим обладнанням, так і з різноманітним віртуальним обладнанням, а також досвід роботи з досить складними мережами.
4. Комбінована платформа має великі перспективи розвитку. Вона надає можливості створити нові лабораторні роботи з комп’ютерних мереж. Надає можливість проводити дослідження, аналіз ефективності і моніторинг мереж, а також виконувати моделювання при проектуванні мереж. Дослідити безпеку комп'ютерних мереж. Моделювати загрози і вчитися захищатися і ліквідувати наслідки.
5. Методику моделювання можна застосовувати навіть на працюючих мережах, не створюючи їм перешкод і загроз.
6. Платформа має низькі витрати на установку і експлуатацію.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1]В. Григорьев, Виртуальная лаборатория по компьютерным сетям. Днепропетровск, 2011. – Режим доступу: http://muff.kiev.ua/files/books/VirtualLaboratoryforcomputernetworksGrigoriev.pdf
[2]Concept of IoT (Internet of thing) on Cisco Packet Tracer. [Електронний ресурс]. – Режим доступу: http://telecomacadmey.com/concept-iot.
[3]Andrea Finardi IoT Simulations with Cisco Packet Tracer. [Електронний ресурс]. – Режим доступу: https://www.theseus.fi/bitstream/handle/10024/150158/Andrea%20Finardi%20%20Master%20of%20Engineering%20%20Information%20technology.pdf?sequence=1&isAllowed=y.
[4]Приложения GNS3 и Cisco Packet Tracer Student. [Електронний ресурс]. – Режим доступу: https://upweek.ru/prilozheniya-gns3-i-cisco-packet-tracer-student-chto-nam-stoit-set-postroit-narisuem-budem-zhit.
[5]Е. Ольков, Основы gns3. Подключение gns3 к реальной сети. – Режим доступу: http://blog.netskills.ru/2015/12/12-gns3-connect-realnetwork.html.
[6]Как из компьютера сделать роутер? [Електронний ресурс]. – Режим доступу: http://provider.net.ru/static/kak-iz-kompyutera-sdelat-router
[7]Центр Интернета вещей Azure. [Електронний ресурс]. – Режим доступу: https://azure.microsoft.com/ru-ru/services/iot-hub/
[8]А. Соммер, Интернет вещей: Arduino в связке с облаком. [Електронний ресурс]. – Режим доступу: https://habr.com/ru/company/microsoft/blog/343450/
[9]Організація компютерних мереж . Iot в cisco packet tracer. Розумний дім. [Електронний ресурс]. – Режим доступу: http://nickshevtsov.blogspot.com/2017/11/iot-cisco-packet-tracer.html
[10]Edge Интернета вещей Azure. [Електронний ресурс]. – Режим доступу: https://azure.microsoft.com/ru-ru/services/iot-edge /
[11]В. Абрамов та С. Клименко, Базові технології комп’ютерних мереж: навчальний посібник. Київ: Ун-т ім. Б. Грінченка, 2014, с. 264.
[12]В. Абрамов та О. Литвин, Методичні аспекти викладання дисциплін напрямку ‘інтернет речей’, Кібербезпека: освіта, наука, техніка, том 1, номер 1, с. 73-85. https://doi.org/10.28925/2663-4023.2018.1.7385

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (4), 2019
ISSN 2663 - 4023

Vadym O. Abramov
candidate of Technical Sciences (Ph.D.), Associate Professor,
Associate Professor of the Department of Information Technology and Mathematic
Borys Grinchenko Kyiv University, Kyiv, Ukraine
OrcID: 0000-0002-8026-1475
v.abramov@kubg.edu.ua

APPLICATION OF COMBINED MODELS OF COMPUTER NETWORKS IN THE TRAINING PROCESS

Abstract. An overview of computer network simulation tools is being conducted in order to create a methodology for studying the relevant disciplines in higher school. The analysis of positive and negative properties of virtual and physical means of simulation of computer networks is carried out. It is concluded that the best for educational institutions are combined models that are quite budget and allow to compile and study practically unlimited topologies of networks, as well as gain experience with real physical equipment. The analysis of virtual simulation tools shows that they contain the means of interaction of the virtual network with external real equipment. This makes it possible to create a composite platform in which part of the model is virtual and the part is actually physical. This allows budget funds to quickly create models of large numbers of networks and allows students to get more information on working with hardware in conditions close to real industrial networks. The platform of the combined modeling is very convenient to use for researching systems on the Internet of Things. It helps in designing to simulate and explore real-world control systems for a large number of virtual "Smart Things" that are presented in the new Cisco Packet Tracer 7.0 simulator. These virtual things can be controlled from external means of the real world through laptops, tablets, etc. Create realistic control programs and related software for this and adjust them in conditions of maximum approximation to reality. New modeling technologies are the basis for the emergence of new teaching methods that are used at the Kiev University of B. Grinchenko.

Keywords: computer networks, virtual models, real equipment, Internet things; control systems; embedded systems; remote laboratories; teaching method.

REFERENCES

[1]Grigoriev V.M., Virtual laboratory on computer networks. Dnepropetrovsk, 2011. Available: http://muff.kiev.ua/files/books/VirtualLaboratoryforcomputernetworksGrigoriev.pdf
[2]Concept of IoT (Internet of thing) on Cisco Packet Tracer. Available: http://telecomacadmey.com/concept-iot.
[3]Andrea Finardi IoT Simulations with Cisco Packet Tracer. Available: https://www.theseus.fi/bitstream/handle/10024/150158/Andrea%20Finardi%20%20Master%20of%20Engineering%20%20Information%20technology.pdf?sequence=1&isAllowed=y.
[4]GNS3 and Cisco Packet Tracer Student applications. Available: https://upweek.ru/prilozheniya-gns3-i-cisco-packet-tracer-student-chto-nam-stoit-set-postroit-narisuem-budem-zhit.
[5]Olkov E. Fundamentals of gns3. Connect gns3 to the real network. Available: http://blog.netskills.ru/2015/12/12-gns3-connect-realnetwork.html .
[6] How to make a router from a computer? Available: http://provider.net.ru/static/kak-iz-kompyutera-sdelat-router
[7] Azure IoT Center. Available: https://azure.microsoft.com/en-ru/services/iot-hub/
[8]Internet of things: Arduino in conjunction with the cloud Alexey Sommer. Available:: https://habr.com/ru/company/microsoft/blog/343450/
[9]Organizational Computing Systems. Iot in cisco packet tracer. Rosumniy dim. Available: http://nickshevtsov.blogspot.com/2017/11/iot-cisco-packet-tracer.html
[10]Edge Интернета вещей Azure. Available: https://azure.microsoft.com/ru-ru/services/iot-edge /
[11]Abramov V.O., Klimenko S.Yu. Bazi tekhnologii ї komp'nyuterny leastzh: primary school. - K .: Kiev. Univ. B. Grinchenko, 2014.p. 264.
[12]V. Abramov and O. Lytvyn, “Methodological Aspects of the Internet of Things Disciplines Study”, Cybersecurity: Education, Science, Technique, vol. 1, no. 1, pp. 73-85 https://doi.org/10.28925/2663-4023.2018.1.7385.