XIV НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ СТУДЕНТІВ ТА МОЛОДИХ ВЧЕНИХ НАВЧАЛЬНО-НАУКОВОГО ІНСТИТУТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЕРЖАВНОГО УНІВЕРСИТЕТУ ТЕЛЕКОМУНІКАЦІЙ

СУЧАСНІ ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

ЗБІРНИК ТЕЗ

19 травня 2022р

КИЇВ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВОГО ІНСТИТУТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
XIV НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ СТУДЕНТІВ ТА МОЛОДИХ ВЧЕНИХ

СУЧАСНІ ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

19 травня 2022р

ЗБІРНИК ТЕЗ

м. Київ

Науково-технічна конференція «Сучасні інфокомунікаційні технології» Збірник тез. К.ДУТ, 2022 – 97 с.

Даний збірник містить тези учасників конференції, представлених на XIV Науково-технічній конференції студентів та молодих вчених інституту Інформаційних технологій «Сучасні інфокомунікаційні технології», яка проводилась 19 травня 2022р. в Державному університеті телекомунікацій, м.Київ.

Робоча мова конференції – українська.

У збірнику представлені тези доповідей XIV Науково-технічної конференції студентів та молодих вчених інституту Інформаційних технологій «Сучасні інфокомунікаційні технології». Розглянуті сучасні проблеми розвитку науки і техніки та визначено шляхи їх вирішення.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Державний університет телекомунікацій
Навчально-науковий інститут інформаційних технологій

ПРОГРАМНИЙ КОМІТЕТ

Бондарчук А. П.– д.т.н., професор, директор Навчально-наукового інституту інформаційних технологій Державного університету телекомунікацій

Вишнівський В. В.– д.т.н., професор, завідувач кафедри Комп'ютерних наук Державного університету телекомунікацій

Жебка В.В.– д.т.н., доцент, завідувач кафедри Технологій цифрового розвитку Державного університету телекомунікацій

Зінченко О.В.– д.т.н., доцент, завідувач кафедри Штучного інтелекту Державного університету телекомунікацій

Негоденко О. В.– к.т.н., завідувач кафедри Інженерії програмного забезпечення Державного університету телекомунікацій

Ткаченко О. М.– д.т.н., доцент, завідувач кафедри Комп'ютерної інженерії Державного університету телекомунікацій

Сторчак К. П.– д.т.н., професор, завідувач кафедри Інженерії програмного забезпечення автоматизованих систем Державного університету телекомунікацій

Вчений секретар
Полоневич О.В.
nevdachinaolya@i.ua

ЗМІСТ

Кухаренко Ю.Д.,
студент 4 курсу, групи ПД-41,
Державного університету телекомунікацій,
(066) 853 43 22, lifehak007@gmail.com
Науковий керівник: Трінтіна Наталія Альбертівна,
кандидат технологічних наук, доцент кафедри Інженерії програмного забезпечення
Державного університету телекомунікацій, м. Київ

РОЗРОБКА СИСТЕМИ КОНТРОЛЮ УСПІШНОСТІ СТУДЕНТІВ

В сучасному світі кожного дня кількість інформації, яку необхідно зберігати росте в геометричній прогресії, набуваючи величезних розмірів.

Саме в цей час з'явилися системи автоматизації, які допомагають людям у структуруванні та зберіганні інформації різного роду, взаємодії між ролями користувачів, тощо.

Мета дослідження. Виходячи з актуальності явища систем автоматизації, було вирішено розробити систему контролю успішності студентів у вигляді веб-сервісу, який буде задовольняти потреби сучасного користувача.

Постановка задачі. Вимоги до веб-сервісу: простота в освоєнні та інтуїтивна зрозумілість у використанні; повнота функціоналу; використання сучасних технологій і фреймворків у створенні сервісу задля його гнучкості та легкості у масштабуванні.

Особливості проетку: зручний інтерфейс з дотриманням всіх правил коректного UI/UX дизайну. Використання універсального фреймворку для веб розробки Java Spring Framework. Доступ до сервісу в режимі онлайн без необхідності будь-яких завантажень на комп'ютер.

Результати дослідження. З огляду на поставлені цілі і складність сервісу, найкращим рішенням буде використання Spring Framework, який у повному обсязі надає функціонал для створення веб-сервісів такого типу. Розроблені на Java проекти легко піддаються масштабуванню і розширенню функціоналу, без необхідності переписувати код.

Дизайн сервісу розроблений в рамках мінімалізму, що робить його простішим для освоєння. Для зберігання даних було обрано базу даних MySQL – найпопулярнішу реляційну СУБД, яка чудово інтегрується в проекти і має простір для оптимізації запитів. Отже, проект включає наступні елементи:

- Сучасна платформа розробки.
- Зручний UI/UX дизайн.
- Потужну базу даних.
- Широкий функціонал.
- Робота в браузері без завантажень.

Далі будуть наведені скріншоти розділів даного проекту.

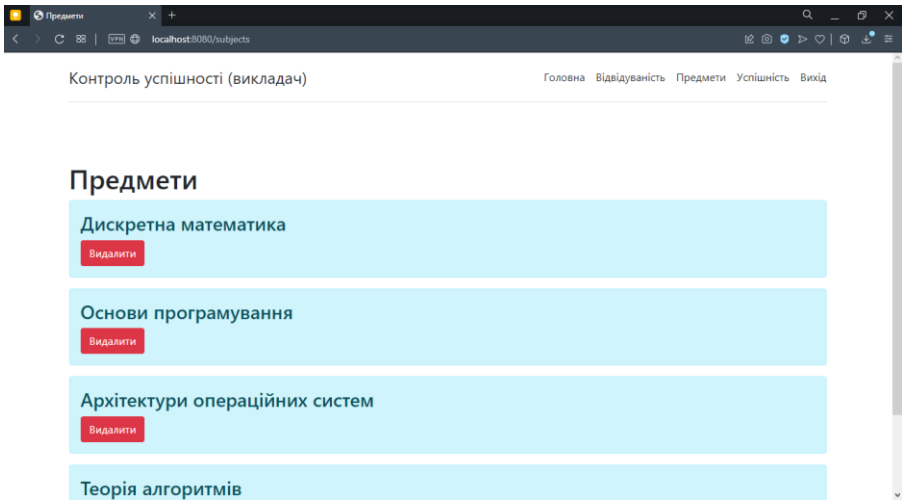

Рис.1 Сторінка «Предмети»

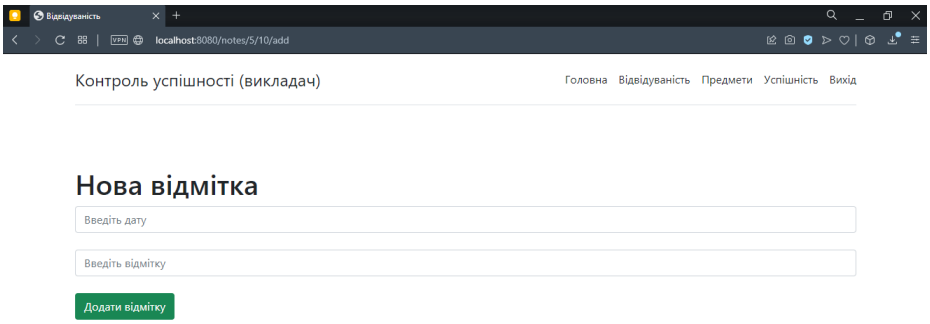

Рис. 2 Сторінка «Відвідуваність»

Висновки та перспективи. Рішень, які повноцінну перекривають поняття «системи контролю успішності» як таких не існує у відкритому доступі. Зазвичай, під даним заголовком публікуються рішення, які за своєю суттю є або електронними журналами, або системами створення тестувань з різних тем.

Виходячи з цього, даний веб-сервіс має практичну цінність, як безкоштовний продукт, який надає функціонал для вирішення вищевказаної проблеми. Основною перевагою розробленого проекту є об’єднання уже існуючих, але доступних в різних сервісах, рішень в одному місці.

Список використаних джерел:

1. Веб сайт: https://habr.com/ru/post/490586/
2. Веб сайт: https://ru.wikipedia.org/wiki/MySQL
3. Веб сайт: https://habr.com/ru/post/321312/

Герасименко Дмитро Олександрович,
студент 4 курсу, групи КІД-42
Державного університету телекомунікацій
(093) 592 33 82, dima.gerasimenko2001@gmail.com
Науковий керівник: Бученко Ігор Анатолійович,
асистент кафедри Комп’ютерної інженерії
Державного університету телекомунікацій, м. Київ

КЛІЄНТСЬКА ВІРТУАЛІЗАЦІЯ

Анотація. *В даній роботі розглянуто питання віртуалізації, розкрито її зміст та вплив віртуалізації на користувачів. Зосереджено увагу на зручності використання клієнтської віртуалізації, перевагах та недоліках, заощадженні часу і захисту під час використання.*

Постановка задачі. Аналіз інформації та формування висновків, щодо користі технології клієнтської віртуалізації над методом розгортання фізичних робочих столів.

Мета дослідження. Дослідити технологію клієнтської віртуалізації.

Результати дослідження. Віртуалізація — це процес створення програмної (віртуальної) версії комп'ютера з виділеними ресурсами центрального процесора, оперативної пам'яті та сховища, які "запозичуються" у фізичного комп'ютера (наприклад, персонального комп'ютера) та/або віддаленого сервера, наприклад, сервера в центрі обробки даних постачальника хмарних послуг.

Віртуальна машина – це комп'ютерний файл (зазвичай його називають образом), який діє як звичайний комп'ютер. Вона може працювати у вікні як окреме обчислювальне середовище (часто для запуску іншої операційної системи) або навіть як ціла система, як це часто реалізується на робочих комп'ютерах. Віртуальна машина відокремлена від решти системи, тобто програмне забезпечення віртуальної машини не може втручатися в роботу основної операційної системи комп'ютера.

Клієнтська віртуалізація, яку також називають віртуалізацією робочих столів, використовує архітектуру мережі клієнт-сервер, щоб зменшити кількість фізичних настільних комп’ютерів, необхідних для розміщення всіх користувачів компанії. Віртуалізація клієнта імітує робочий стіл користувача, але відокремлює робочий стіл від обладнання, ОС і програм. Імітований робочий стіл клієнта або віртуальна машина (VM) працює на фізичному хост-сервері, на якому запущено програмне забезпечення віртуалізації, ядро якого називається гіпервізором. Багато віртуальних клієнтів можуть працювати на одному хост-сервері, кожен клієнт має різні властивості користувача, дані, програми і навіть ОС. Це дозволяє користувачам безперешкодно отримувати доступ до своїх звичайних настільних комп’ютерів з недорогих комп’ютерів низького класу, тонких клієнтів або спільних комп’ютерів.

Ця централізація обчислень за допомогою віртуалізації клієнтів допомагає відділам інформаційних технологій знизити витрати на апаратне забезпечення та дозволяє налаштовувати нові настільні комп’ютери за лічені хвилини, що заощаджує також час. Це також спрощує завдання оновлення

клієнтських комп’ютерів за допомогою оновлень програмного забезпечення, виправлень безпеки та визначення вірусів, що звільняє IT-персонал для виконання інших важливих завдань. Віртуалізація комп’ютерного клієнта особливо корисна в середовищах тестування або розробки. Це дозволяє системним адміністраторам і розробникам програмного забезпечення встановлювати та тестувати програми, ізольовані від інших машин, таким чином не піддаючи ризику свої мережі.

Для користувачів віртуалізація пропонує більш гнучкі обчислення. Ця технологія дозволяє їм безпечно отримувати доступ до своїх програм і даних з будь-якого місця в їхній локальній мережі (LAN), глобальній мережі (WAN) або звідусіль, де вони можуть отримати доступ до Інтернету. Крім того, оскільки IT може вирішувати більшість проблем клієнтських програм централізовано, користувачі можуть отримати вигоду від меншого простою.[1]

Термінальний сервер, сервер терміналів (terminal server) – сервер, що надає клієнтам обчислювальні ресурси (процесорні ядра, пам'ять, дисковий простір) для вирішення завдань. Технічно термінальний сервер є дуже потужним комп'ютером або кластером, з'єднаним по мережі з термінальними клієнтами - які, як правило, є малопотужними або застарілими робочими станціями, або спеціалізованими рішеннями для доступу до термінального сервера. Термінальний сервер служить для віддаленого обслуговування користувача з робочим столом.

Переваги використання термінального сервера:

- зниження витрат на адміністрування;
- підвищення безпеки та зниження ризику інсайдерських зломів;
- зниження витрат на програмне та апаратне забезпечення;
- зниження витрати електроенергії.

Недоліки використання термінального сервера: концентрація всієї функціональності в рамках одного сервера; негативні наслідки для користувачів при критичних помилках сервера; проблеми з ліцензуванням додатків, що використовуються декількома користувачами одночасно.[2]

Висновки та перспективи. Віртуалізація має великий потенціал для компаній та їх обчислювальної інфраструктури. Це дозволяє компаніям надавати високодоступний, безпечний і гнучкий доступ до критично важливих даних і додатків без фінансових витрат і витрат енергії на традиційне фізичне середовище робочого столу. Зазвичай саме великі компанії отримують найбільшу вигоду від віртуалізації.

Список використаних джерел:

1. Онлайн-енциклопедія Netinbag [Електронний ресурс]: [Веб-сайт]. – Електронні дані. – Сполучені Штати Америки : Netinbag, 2007. – Режим доступу: www.netinbag.com (дата звернення 17.05.2022) – Що таке віртуалізація клієнтів?

2. Онлайн-енциклопедія Вікіпедія [Електронний ресурс]: [Веб-сайт]. – Електронні дані. – Маямі, Флорида : Wikipedia, 2001. – Режим доступу: www.uk.wikipedia.org (дата звернення 17.05.2022) – Термінальний сервер.

Іщенко Ілля Євгенович,
студент 4 курсу, групи ТСД-42
Державного університету телекомунікацій
067-584-93-28, ischenko2012@gmail.com
Науковий керівник: Градобоєва Неля Вікторівна,
к.т.н., доцент кафедри телекомунікаційних систем та мереж
Державного університету телекомунікацій, м. Київ

ЯК 5G URLLC І ПЕРИФЕРІЙНІ ОБЧИСЛЕННЯ МОЖУТЬ ЗРОБИТИ РОЗУМНІШІ ФАБРИКИ

Постановка задачі. Дослідження актуальних новин у сфері комп'ютерних наук.

Мета дослідження. Пошук, вивчення, перевірка актуальності та правдивості інформації, її дослідження та оприлюднення цієї інформації у роботі.

Результати дослідження. 5G приніс багато надій і мрій у телекомунікаційну індустрію, обіцяючи постачальникам комунікаційних і цифрових послуг спосіб відкрити нові потоки доходу та моделі монетизації. Проте для більшості це не вдалося. Тепер це може змінитися. Завдяки 5G URLLC і граничним обчисленням, телекомунікації можуть стати основним фактором автоматизації виробництва на основі мереж 5G.

Що робить завод розумним? Існує суттєва різниця між традиційними фабриками та концепцією розумної фабрики. Хоча обидва стосуються фізичного місця, де відбувається виробництво, спосіб їх роботи дуже різний. Традиційні фабрики потрібно будувати для конкретних компаній з дуже жорсткими вимогами. У більшості випадків вони взагалі не оцифровані, а якщо і є, то на низькому рівні. Концепція розумної фабрики включає в себе оцифровку та використання різних сучасних технологій, включаючи штучний інтелект, машинне навчання, периферійні обчислення. Він дуже гнучкий і адаптується до мінливих потреб свого власника/орендаря.

5G URRLC можна сприймати як зміну гри, коли йдеться про поширення розумних фабрик. Раніше багато додатків IoT не могли обслуговуватися бездротовими технологіями. Такі рішення, як «заводський цех», були виключно в дротовому домені, і до 5G URRLC бездротові технології не могли відповідати цим вимогам. Тепер URLLC 5G може змінити це. 5G має величезний потенціал стати реальним інструментом для більш просунутої автоматизації та оцифровки для Індустрії 4.0. На відміну від попередніх бездротових технологій, завдяки URLLC у поєднанні з MEC, 5G може бути життєздатною альтернативою дротовим заводським рішенням, які вимагають надзвичайної надійності та затримки менше 10 мс. Позбавлення від проводів навіть для статичних заводських складальних ліній забезпечує набагато більшу маневреність у переконфігурації заводського цеху. Це, у поєднанні з новою мережевою архітектурою, дозволяє програмувати ПЛК та реалізовувати хмарні обчислення, що потім сприяє більш просунутому програмному забезпеченню для автоматизації виробничих систем.

Постачальники послуг зв'язку та цифрових послуг, зробивши величезні

інвестиції в 5G, очікують, що це поверне користь зі значним збільшенням доходу. Це можливо, особливо якщо мова йде про розумні фабрики, але оператори повинні правильно визначити свою стратегію. Деякі, можливо, захочуть підійти до мегафабрик — великих гравців з великою кількістю місць у різних місцях. Це може здатися гарною ідеєю, але це може бути складно. Мегафабрики мають фінансові ресурси для внутрішнього розгортання рішень, без залучення посередників, таких як оператор.

Список використаних джерел:

1. 5G. [Електронний ресурс]//Режим доступу: https://ru.wikipedia.org/wiki/5G
2. Розумні фабрики. [Електронний ресурс] // Режим доступу: https://www.it.ua/knowledge-base/technology-innovation/smart-factory

Грищенко Ярослав Олександрович
Студент 5 курсу, групи БСДМ-53
(068) 6566732, grischenckokgtl@gmail.com
Науковий керівник: Довженко Надія Михайлівна
к.т.н., доцент кафедри Інформаційної та кібернетичної безпеки
Державного університету телекомунікацій, м. Київ

ДОСЛІДЖЕННЯ ПРОЦЕСІВ ЗАХИСТУ ІНФОРМАЦІЇ В IoT

Анотація. *Розглядаються процеси захисту та обміну інформації між пристроями систем Інтернету речей та мережею Інтернет, а також основних методів та засобів передачі інформації та їх подальше удосконалення та стандартизація з точки зору безпеки, зроблено дослідження корпорації HP, метою якого було не виявити якісь конкретні небезпечні інтернет-пристрої і викрити їх виробників, але позначити проблему ІБ-ризиків в світі IoT в цілому. Проведено аналіз та оцінку ризиків при використанні систем інтернету речей. Дані системи знаходяться на тісному стику інженерії програмного забезпечення та комп'ютерної інженерії.*

Постановка задачі. Науковою задачею даних досліджень є забезпечення безпечного обміну інформацією між пристроями систем Інтернету речей та мережею Інтернет. Задача є актуальною, оскільки зараз аналітики оцінюють число активних IoT-пристроїв у 27 мільярд, то через чотири роки їх кількість перевищить 50 мільярдів. У зв'язку з розвитком IoT-технологій висловлюють занепокоєння фахівці у сфері інформаційної безпеки. На їхню думку, величезна кількість погано захищених інтернет-девайсів дає нові можливості кіберзлочинцям, яким уже вдалося зламати ряд IoT-систем [1].

Мета дослідження. Метою роботи є аналіз існуючих методів та засобів передачі інформації у системах Інтернету речей та їх подальше удосконалення та стандартизація з точки зору безпеки. Аналіз безпеки в IoT є важливим, так як кінцеві суб'єкти мають довіряти технології. Унікальність полягає в тому, що повинні відбуватися автентифікація, авторизація кінцевого обладнання, зберігання та обробка інформації, в тому числі і конфіденційної та критично важливою.

Результат дослідження. Недавнє дослідження корпорації HP, метою

якого було не виявити якісь конкретні небезпечні інтернет-пристрої і викрити їх виробників, але позначити проблему ІБ-ризиків в світі IoT в цілому, звертають увагу на проблеми як з боку власників пристроїв, так і на проблеми, над усуненням яких повинні працювати розробники. Так, на самому початку експлуатації користувачеві обов'язково потрібно замінити фабричний пароль, встановлений за замовчуванням, на свій особистий, оскільки фабричні паролі однакові на всіх пристроях і не відрізняються стійкістю. Оскільки не всі прилади мають вбудовані засоби ІБ-захисту, власникам також слід подбати про встановлення зовнішнього захисту, призначеного для домашнього використання, щоб інтернет-пристрої не стали відкритими шлюзами в домашню мережу або прямими інструментами заподіяння шкоди. яка надходить до них поза волею власника [2, с.50].

У ході проведеного дослідження також виявлено, що приблизно в 70% проаналізованих пристроїв не шифрується бездротовий трафік. Веб-інтрефейс 60% пристроїв експерти HP вважають небезпечним через недосконалу організацію доступу і високий ризик міжсайтового скриптингу. У більшості пристроїв передбачені паролі недостатньої стійкості [3, с.149]. Приблизно 90% пристроїв збирають ту чи іншу персональну інформацію про власника без його відома. Всього ж фахівці HP нарахували близько 25 різних вразливостей у кожному з досліджених пристроїв і їх мобільних та хмарних компонентах.

Були виділені такі слабкі місця IoT:

- ✓ перехід на IPv6;
- ✓ використовуючи слабкість одного гаджета, хакеру легко потрапити в усю мережу;
- ✓ стандартизація архітектури і протоколів, сертифікація пристроїв;
- ✓ інформаційна безпека;
- ✓ стандартні облікові записи від виробника, слабка аутентифікація;
- ✓ відсутність підтримки з боку виробника для усунення вразливостей;
- ✓ використання незахищених мобільних технологій.

Висновки та перспективи. Проведено аналіз та оцінку ризиків при використанні систем інтернету речей. Дані системи знаходяться на тісному стику інженерії програмного забезпечення та комп'ютерної інженерії. Тому для подібних досліджень необхідним є як вивчення принципів роботи IoT-пристроїв, так і способів мережевого обміну даними. Оскільки такі системи мають застосування у всіх сферах життя, безпека обміну даними має бути одним із найголовніших аспектів даної галузі.

Список використаних джерел:

1.Rosencrance L. Internet of things (IoT) [Електроний ресурс]/L. Rosencrance, S. Sharon, I. Wigmore–Режим доступу до ресурсу: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

2. Васильев Г. Интернет вещей и информационная безопасность / Г. Васильев.// Первая миля. – 2016. – №6. – С. 50–55.

3. Лоднева О.Н. Анализ трафика устройств Интернета вещей/О.Н.Лоднева,Е.П. Ромасевич.//Современные информационные технологии и ИТ-образование.–2018.–№1.–С. 149–169.

Іванюк Валерія Олександрівна,
Студент 4 курсу, групи ПД-42
Державний університет телекомунікацій
(066) 250 14 78, ler0nvelr0n@gmail.com
Науковий керівник: Коба Андрій Борисович,
старший викладач кафедри Інженерії програмного забезпечення
Державного університету телекомунікацій, м. Київ

АКТУАЛЬНІСТЬ ГРИ ЖАНРУ «ТРИ В РЯД» В СУЧАСНІЙ ІГРОВІЙ ІНДУСТРІЇ

Анотація. *На сьогоднішній день багато людей полюбляють встановлювати ігри на свої смартфони, особливо на смартфони, що використовують операційну систему IOS. З розповсюдженням смартфонів, кількість ігор стрімко зростає, Ігри в жанрі «три в ряд» набирають оборотів і стають популярними в наш час.*

Результат дослідження. Ринок комп'ютерної індустрії є самою масштабною частиною світового ринку. 2021 рік став найбільшим в історії з продажів комп'ютерних ігор. Ігровий ринок досяг $ 106,6 млрд і аудиторії в 2,2 млрд геймерів по всьому світу.

Одним з найбільших сегментів даного ринку є ніші багатокористувальних ігор, представлених в великій кількості різних жанрів. Серед цих жанрів перспективним і популярним є «три в ряд».

До особливостей, що роблять ігри в жанрі "три в ряд" такими популярними можна віднести:

- Рівні. Найпозитивнішими емоціями є завдання подолати рівні та відчуття виконаного завдання.
- Візуальні зображення – Багато гравців не заперечують, що деякі ігри присвячені одному і тому ж сюжету. Вони насолоджуються відчуттям, яке вони мають від гарного мистецтва та цікавих рівнів.
- Історія – зараз є багато ігор, які додають шар історії поверх відповідної механіки. Наприклад, Gardenscapes є чудовим прикладом.
- Мета-гра – деякі ігри використовують механіку відповідності як просту, але дуже гнучку механіку для основного ігрового процесу. Ігри RPG є чудовим прикладом.
- Хронометраж – деякі ігри розраховані на час. Нові плитки безперервно додаються, і гравець змушений складати матчі до того, як поле заповниться.

Ще одна причина, чому даний жанр ігор настільки успішний, полягає в тому, що ці ігри, як правило, легко продати. Більшість великих програм також витрачають значні кошти на залучення користувачів і платні маркетингові кампанії. Ці рекламні зусилля також можуть сприяти їхньому величезному успіху.

Щоб підкреслити масштаб цих ігор: згідно з повідомленням у блозі Sensor Tower, у 2018 році у серії King’s Candy Crush гравці витрачали в середньому 4,2 мільйона доларів на день, що перевищило загальну суму

франшизи за 1,5 мільярда доларів.

На основі цих даних можна зробити висновок, що ігри жанру «три в ряд» залишаються актуальними і сьогодні. А розробка даної гри на платформу iOS може бути прибутковою і перспективною ідеєю.

Список використаних джерел:

1. Why the Match 3 games are so popular [Електронний ресурс]. - Режим доступу: https://gamingonphone.com/editorial/why-the-match-3-puzzle-games-are-so-popular/
2. Chain shot game [Електронний ресурс]. - Режим доступу: https://en.wikipedia.org/wiki/SameGame
3. Sensor Tower, King's Candy Crush [Електронний ресурс]. - Режим доступу: https://app.sensortower.com/android/us/king/app/candy-crush-saga/com.king.candycrushsaga/overview

Ігнатова М.В.
студентка 4 курсу, групи ПД-41
Державного університету телекомунікацій
(093)5872315, ignatova.mv2601@gmail.com
Науковий керівник: Дібрівний О.А.,
доктор філософії, викладач кафедри Інженерії програмного забезпечення
Державного університету телекомунікацій, м. Київ

ЗАСОБИ ДЛЯ СТВОРЕННЯ ВІЗУАЛЬНИХ НОВЕЛ

Постановка задачі. Дослідити існуючі засоби для створення візуальних новел.

Мета дослідження. Дослідити існуючі засоби для розробки майбутнього програмного продукту у вказаному жанрі.

Результат дослідження. Ігровий двигун - це фундамент майбутнього проекту, його ядро. Програмний код на основі якого будуть з'являтися нові версії гри, доповнення або навіть ще якісь нові проекти схожі за жанром.

Найбільш використовуваними ігровими двигунами для розробки візуальних новел можна вважати Unity та Ren'Py.

Ren'Py - безкоштовний ігровий двигун ,що був зроблений спеціально для розробки візуальних новел. Вийшов у 2004 році, остання версія 2.4.11 вийшла у 2021. Підтримує кросплатформеність.Для розробки продукту використовується Python.

З останніх розроблених на цьому двигуні візуальних новел можна назвати: **"**Doki-Doki High School Love Time", "Let's Go! Hiragana", "Tour de Pharmacy", "Life goes on"та інші.

Ігровий двигун дозволяє запустити готовий шаблон проекту. В якому вже є основні елементи гри. Розробнику залишається на основі вже готового проекту створити свою гру. Для редагування коду ігровий рушій рекомендує або вже інстальовані середовища розробки, або невеликий список з безкоштовних , що підтримують Python.

У 2005 році світ побачив новий кросплатформений ігровий двигун - Unity. На сьогоднішній він підтримує більше 25 платформ. Рушій

використовують для розробки 2D та 3D ігор, а також для додатків доповненої реальності. Мовою для розробки додатків на основі цього двигуна є C#.

Двигун Unity також підтримує встановлення розширень для полегшення розробки конкретних жанрів ігор. Візуальни новели не виключенням. Прикладами розширень для розробки гри в цьому жанрі можна вважати: Naninovel, Visual Novel Toolkit та Fungus.

Naninovel - це платне повноцінне розширення для створення візуальних новел. Має відкритий код, кросплатформений, додаткові вікна для роботи з сюжетом та сценами гри, спрощений варіант для прописування скриптів візуальної новели. Також розробнику надаються вже готові шаблони для реалізації налаштувань гри, головного меню, вікна з текстом та інше.

Visual Novel Toolkit - безкоштовне розширення для розробки візуальної новели на ігровому двигуні Unity.

Це розширення дозволяє створювати структуру ієрархії сюжету візуальної новели, спрощує керування об’єктами, надає готовий механізм діалогів, мінімальну кількість аудіозаписів для гри та свій шаблон інтерфейсу гри.

Fungus - також безкоштовне розширення для створення візуальних новел. Надає можливість зручної організації варіативності візуальної новели та структуризації історії.

Отже було розглянуто різні засоби для розробки візуальних новел, їх особливості та характеристики. В майбутньому це може бути використано для вибору ігрового рушія для створення власного продукту.

Список використаних джерел:

1. Офіційний сайт рушія Ren'Py [Електронний ресурс]: [Веб–сайт]. – електронні дані. – Режим доступу: https://www.renpy.org
2. Офіційний сайт рушія Unity [Електронний ресурс]: [Веб–сайт]. – електронні дані. – Режим доступу: https://docs.unity3d.com
3. Офіційний сайт розширення для Unity Naninovel[Електронний ресурс]:[Веб–сайт]– електронні дані.– Режим доступу: https://naninovel.com
4. Офіційний сайт розширення для Unity Fungus[Електронний ресурс]: [Веб–сайт]. – електронні дані. – Режим доступу: https://fungusgames.com

Ведмідь Д.Т.
студент 4 курсу, групи ТСД-41
Державний університет телекомунікацій
Науковий керівник: Марков С.Ю.
К.т.н., доцент кафедри Телекомунікаційних систем та мереж
Державного університету телекомунікацій, м. Київ

ОСОБЛИВОСТІ ПРОЕКТУВАННЯ ПАСИВНИХ ОПТИЧНИХ МЕРЕЖ

Наразі на мережах доступу волоконно-оптичні лінії в основному застосовуються як елемент гібридної мідно-волоконної лінії. Але є вже мережі доступу, в яких мідні проводи відсутні, а є тільки оптичні волокна. Це пасивні

оптичні мережі. Технологія пасивних оптичних мереж представляє особливий інтерес в плані розширення сфери застосування цифрових широкосмугових мереж. Застосування цієї технології для побудови комп'ютерних мереж є найбільш прийнятним рішенням для локальних комп'ютерних мереж [1].

На сьогодні існує необхідність вдосконалення проектування, будівництва та експлуатації пасивних оптичних мереж з метою побудови мереж з оптимальними характеристиками, тому проектні дослідження комп'ютерних мереж, побудованих з застосуванням оптичних технологій є актуальними.

Основні проблеми, які необхідно вирішувати при проектуванні:

- визначення коефіцієнту проникнення інтернету;
- обрання топології мережі на основі відомостей про територію місцевості, де проектується мережа;
- обрання технології GPON, EPON або WDM-PON;
- обрання обладнання, комплектуючих елементів і кабелів;
- визначення місць розташування сплітерів, боксів та коробок;
- обрання трас кабелю, його ємності з урахуванням резервування;
- розрахунок бюджету оптичної потужності та бюджету загасання [2,3].

В роботі розглянуто методологію вирішення задач, що вказані вище. Розглянуто методи визначення коефіцієнту проникнення на основі загальних статистичних даних по країні, даних по регіону проектування та одержання даних безпосередньо шляхом опитування. Порядок обрання топології мережі визначається шляхом аналізу розташування потенціальних користувачів по території району, де проектується мережа.

Обрання технології передачі та відповідного обладнання базується на аналізі вимог, що поставлені перед проектувальником. Ці вимоги: максимальна дальність зв'язку, кількість користувачів та щільність їх розташування, мінімізація витрат на обладнання. Наразі вирішення цієї задачі значно спрощене завдяки тому, що на ринку телекомунікаційного обладнання є обладнання, яке дозволяє використовувати як технологію GPON, так і технологію EPON.

На прикладі проектування PON конкретного району показане застосування методів вирішення задач проектування пасивних оптичних мереж, проведений розрахунок оптичного бюджету та економічних характеристик мережі.

Список використаних джерел:

1. Зингеренко Ю.А. Пассивные оптические сети xPON. Учебное пособие/Ю.А. Зингеренко. – Санкт-Петербург: ИТМО, 2020. – 156 с.

2. Петренко И.И. Пассивные оптические сети PON. Часть 1. Архитектура и стандарты /*И.И.* Петренко, Р.Р. Убайдуллаев // Lightwave Russian Edition. – 2004. - № 1. - С. 22-31.

3. Петренко И.И. Пассивные оптические сети PON Часть 2. Ethernet на первой миле/ И.И. Петренко, Р.Р. Убайдуллаев // Lightware Russian edition. – 2004. - № 2. – С. 48-56.

Полодюк А.В.
Студентка 5 курсу, групи ТСЗ-51
Науковий керівник: Марков С.Ю.
К.т.н., доцент кафедри Телекомунікаційних систем та мереж
Державного університету телекомунікацій, м. Київ

СУЧАСНІ ЗАДАЧІ ПРОЕКТУВАННЯ ЗОНОВИХ МЕРЕЖ УКРАЇНИ

В Україні ще є достатня кількість систем передачі, що працюють по мідним кабелям, або по оптичним з обладнанням PDH. Однак наразі швидко зростають вимоги до такої якості зв'язку, яку вказані системи забезпечити не можуть. Альтернативним рішенням є застосування обладнання SDH [1]. Це обладнання має більш високу швидкість передачі та більш високу надійність зв'язку, зокрема завдяки можливості резервування, що забезпечується застосуванням надійної топології мережі.

Найбільш надійною для використання в комп'ютерних мережах та в мережах зв'язку є кільцева топологія, завдяки якої створюються резервні шляхи та підвищується надійність зв'язку.

В роботі проведене дослідження проблем зонового зв'язку України. Показана актуальність та перспективність реконструкції зонових мереж окремих областей країни з метою заміни обладнання, що працює по мідним кабелям, та самих цих кабелів на сучасні цифрові системи передачі технології SDH. В тих випадках, в яких зв'язок організований по оптичному кабелю, але з застосуванням технології PDH, теж доцільна заміна обладнання на більш прогресивне обладнання синхронної ієрархії.

На конкретному прикладі існуючої зонової мережі розроблений проект її реконструкції з заміною на однієї з ділянок мідного кабелю та відповідного обладнання на одномодовий оптичний кабель з системою передачі SDH, а також з заміною на іншої ділянці застарілої системи передачі PDH на систему передачі SDH. При здійсненні цих замін проект передбачає створення кільцевої мережі.

При створенні кільцевої мережі проведений розрахунок кількості первинних цифрових потоків Е1 на сегментах мережі, що дозволяє визначити рівень синхронної цифрової ієрархії для мережі. На сегментах визначена потреба в швидкості для організації телефонного зв'язку, а також для передачі даних (інтернет) [3].

Проведена економічна оцінка проектних рішень, яка показує ефективність вкладених інвестицій для створення мережі за цім проектом. Строк окупності проекту з урахуванням дисконтування не перевищує встановлених галузевих нормативів.

Список використаних джерел:

1. Грицуленко С.И. Украинский рынок телекоммуникационных услуг в контексте стратегии поведения его участников в условиях цифровой трансформации экономики и социума / С.И. Грицуленко, А.И. Джигалюк // Бизнес Информ. – 2019. - № 11. – С. 194-203.

2. Скляров О.К. Волоконно-оптические сети и системы связи: Учебное пособие. 2 изд., стер. / О.К. Скляров. - Лань, СПб. - 2010. – 272 с.

3. Арифметика интернета [Електронний ресурс] //– Режим доступу/ https://tel-sis.ru/blog/arifmetika-gpon/.

Якимчук Ю.О.
Студент 5 курсу, групи ТСЗ-51
Науковий керівник: Марков С.Ю.
К.т.н., доцент кафедри Телекомунікаційних систем та мереж
Державного університету телекомунікацій, м. Київ

ПРОБЛЕМИ ПРОЕКТУВАННЯ ЦИФРОВИХ РАДІОРЕЛЕЙНИХ ЛІНІЙ

Протягом багатьох років одним з найбільш економічних і швидких способів організації передачі інформаційно-транспортних потоків на великі відстані залишається радіорелейний зв'язок (РРЗ). Раніш в основному апаратура лінії такого зв'язку була аналоговою, зараз їй на зміну прийшли сучасні цифрові радіорелейні станції (ЦРРС), що мають високу пропускну здатність. Їх пропускна здатність складає 155 Мбіт/с і більш, а передача сигналів ведеться з використанням багатопозиційних видів модуляції. Для сучасних ЦРРС характерна наявність системи теле обслуговування, яка програмно підтримує рівень управління мережними елементами і мережею та забезпечує контроль, управління і технічне обслуговування устаткування [1].

При проектуванні цифрових ліній РРЗ вирішуються наступні задачі [2]:

- вибір діапазону частот, в якому працюватиме лінія;
- вибір обладнання станцій;
- вибір розташування проміжних станцій та частотного плану;
- розрахунок висот підвісу антен;
- розрахунок якісних характеристик лінії та характеристик надійності;
- економічне обгрунтування проектних рішень.

В роботі проведений аналіз вирішення основних задач проектування. Вибір діапазону частот обумовлений в основному відстанню між станціями, тому що випромінювання різних частот поширюється та ослабляється по різному. Станційне обладнання в значної мірі пов’язане з обраним діапазоном частот. Розташування проміжних станцій має забезпечити достатню розв’язку між каналами за рахунок використання напрямних властивостей антен. При визначенні висот підвісу антен створена програма розрахунку профілю траси, за допомогою якої з урахуванням розміру зони Френзеля знайдені висоти підвісу.

При оцінці якісних характеристик лінії розраховані [3]: імовірність порушення зв’язку, шо викликана дощем; імовірність порушення зв’язку, що викликана інтерференцією радіо променів; враховані завмирання, втрати в атмосфері та явище рефракції; розрахований загальний коефіцієнт неготовності лінії.

На прикладі конкретної траси проведена економічна оцінка проектних рішень.

Список використаних джерел:

1. Современная радиорелейная связь/ - [Електронний ресурс] / – 2017 Режим доступу: https://lantorg.com/article/sovremennaya-radiorelejnaya-svyaz / 2017/09/17.

2. Быховский М.А. Основы проектирования цифровых радиорелейных линий связи/ М.А. Быховкий, Ю.М. Кирик, В.И. Носов – М.: Горячая линия-Телеком, 2014. – 334 с.

3. Анализ методов оценки качества сигнала: рекомендации G.821 и G.826/ - [Електронний ресурс] / – 2016 Режим доступу: //http://www.tools.ru/tools/377595.html

Івахненко Маріанна Володимирівна
студентка 5 курсу, групи БСДМ-53
Державного університету телекомунікацій
Григоренко Дмитро Юрійович
студент 5 курсу, групи БСДМ-53
Державного університету телекомунікацій
Науковий керівник: **Довженко Надія Михайлівна**,
к.т.н., доцент, доцент кафедри Інформаційної та кібернетичної безпеки
Державного університету телекомунікацій, м. Київ

СУЧАСНІ ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ. КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Анотація. *Сучасна епоха стала свідком швидкого розвитку комп'ютерних технологій як апаратного, так і програмного забезпечення. Щороку з'являється безліч нових досягнень, від домашньої робототехніки до передових операційних систем, мікропроцесорів та суперкомп'ютерів із величезними обчислювальними можливостями. Загалом значний обсяг роботи у цій галузі виконується IT-спеціалістами. Вони невпинно працюють над створенням нового програмного забезпечення та комп'ютерного обладнання для використання в різних програмах.*

Область обчислювальної техніки існує з тої пори, як були розроблені перші комп'ютери. Насправді люди, які розробили антикітерський механізм тисячі років тому, могли б вважати себе одними з перших комп'ютерних інженерів, оскільки вони розробили апаратне забезпечення, яке стало основою всіх обчислювальних систем, які ми використовуємо і розуміємо сьогодні.

З того часу область комп'ютерної інженерії значно зросла і розвинулася, надавши широкий спектр технологічних досягнень, які багато людей використовують щодня. Наприклад, комп'ютерні інженери брали участь у розробці:

Смартфонів - включають як апаратне забезпечення, що підтримує операційну систему, так і саму операційну систему.

Бездротові мережі - дозволяє світові використовувати Інтернет

Робототехніка - може бути розроблена як особистого, так і промислового використання.

Принципи обчислювальної техніки можуть застосовуватися для інших цілей, включаючи розробку інтегральних схем, вбудованих систем, комп'ютерного зору, архітектури комп'ютерних систем і багато іншого.

На перший погляд, комп'ютерна інженерія може здатися вузькою областю з єдиною метою. Однак комп'ютерна інженерія може бути розбита на безліч різних підкатегорій, кожна з яких орієнтована на конкретну спрямованість. Хоча було б неможливо перерахувати всі підтеми в області комп'ютерної інженерії, наведений нижче список пояснює деякі з цих відмінностей:

Вбудовані системи. Вбудовані системи працюють у межах більшої системи та виконують певну функцію, невіддільну частину об'єкта загалом.

Комп'ютерні системи. Підобласть комп'ютерних систем фокусується на розробці процесів, що забезпечують надійність та безпеку комп'ютерних систем.

Бездротові мережі та зв'язок. Ця спеціалізація в основному зосереджена на розробці бездротових мереж та систем зв'язку, а також методів передачі та

зберігання даних.

Комп'ютерні мережі. Це підполе пов'язане з технологією, яка дозволяє кільком комп'ютерам працювати у більшій мережі.

Комп'ютерне кодування. Підкатегорія комп'ютерного кодування фокусується на використанні наявних методів кодування, а також на розробці нових з різними програмами, такими як захист конфіденційної інформації.

Операційні системи. Комп'ютерні інженери в цій галузі працюють над розробкою та покращенням операційних систем.

Робототехніка. Деякі комп'ютерні інженери можуть працювати над розробкою робототехніки, що призначена для громадського або приватного використання.

Є багато переваг бути комп'ютерним інженером. Ось деякі потенційні результати для комп'ютерних інженерів на полі.

Попит: Однією з переваг кар'єри комп'ютерного інженера є те, що, за даними BLS, існує попит по всій країні, що дає можливість комп'ютерним інженерам працювати практично в будь-якому місці.

Конкурентний аналіз: здатність керувати великим обсягом даних та маніпулювати ними сама по собі є конкурентною перевагою. Крім того, складання бюджету, планування та прогнозування - це неймовірно потужний спосіб залишатися попереду конкурентів, він виходить далеко за межі стандартного аналізу, а також легко виконується за допомогою програмного забезпечення BI. Компанії також можуть відстежувати продажі та маркетинг своїх конкурентів та дізнаватися, як диференціювати продукти та послуги.

Інновації та творчість: комп'ютерні інженери працюють над створенням кращих та оптимізованих версій наявних продуктів. Вони повинні враховувати технологічні досягнення, а також тенденції для створення інноваційних рішень, що може бути дуже цікавим для професіоналів, які люблять йти в ногу з часом і отримувати задоволення від розв'язання проблем.

Список використаних джерел:

1. WHAT IS COMPUTER ENGINEERING? [Електронний ресурс] – Режим доступу до ресурсу: https://www.onlineengineeringprograms.com/faq/what-is-computer-engineering.

2. Computer Engineering [Електронний ресурс] – Режим доступу до ресурсу: http://ccecc.acm.org/guidance/computer-engineering#:~:text=Computer%20engineering%20is%20defined%20as,systems%20and%20computer%2Dcontrolled%20equipment.

Шрам Максим Миколайович
аспірант 1 курсу, групи АКІ-123
Державного університету телекомунікацій, м. Київ
(097)1185542, dut.maxim@gmail.com
Науковий керівник: Ткаченко Ольга Миколаївна,
доктор технічних наук, професор,
завідувач кафедри Комп'ютерної інженерії
Державного університету телекомунікацій, м. Київ

АТАКИ НА БЕЗДРОТОВІ МЕРЕЖІ ТА ЇХ ВИЯВЛЕННЯ

Анотація. *На сьогоднішній день питання безпеки бездротових мереж є актуальними через їхнє повсюдне поширення. Безпека бездротових систем полягає у запобіганні несанкціонованому доступу або заподіянню шкоди комп'ютерам із боку зловмисників. Ризики, пов'язані з використанням мереж WLAN, коливаються від прослуховування до націлених внутрішніх атак, а також атак, спрямованих на зовнішні сайти.*

Бездротові мережі стали невід'ємною частиною нашої діяльності. Вони спрощують багато процесів, практичні та швидкі, проте, з іншого боку, не секрет, що бездротові мережі більш уразливі для атак та зловмисників. Акти проникнення та вторгнення, відомі як атаки на бездротові мережі, націлені на бездротові мережі, є серйозними погрозами. Зважаючи на перераховані причини, необхідно знати про види атак і їх наслідки з метою подальшого запобігання та зменшення їх дії.

Атаки на бездротові мережі спрямовані на захоплення інформації, що передається через мережу, та вторгнення в інформаційний трафік.

Розглянемо найбільш популярні атаки. Атаки типу – людина посередині. Як правило, атаки виду «людина посередині» поділяються на два види: підслуховування та маніпуляція. Під час прослуховування, зловмисник прослуховує якийсь набір передач між різними хостами, важливо, щоб у цей час комп'ютер зловмисника не був однією зі сторін у з'єднання. Атаки маніпуляції використовують можливість прослуховування, а також захоплення даних з метою подальшої модифікації вмісту.

Одними з популярних серед зловмисників атак стали спуфінг-атаки. Даний вид атак є мережевими атаками, де один учасник маскується під іншого. Найчастіше спуфінг-атаки націлені на вимушення жертви відправляти трафік не безпосередньо легітимному одержувачу, а атакуючому, що ретранслює трафік далі. У випадку IP-спуфінгу переслідується мета переконати жертву, що трафік приходить від легітимного відправника і прийняти чи хоча б просто пропустити його.

Іншими популярними видами атак на бездротові мережі є атаки виду – відмова у обслуговуванні. Метою будь-якої атаки цього виду є створення перешкод для користувача під час підключення до мережевих ресурсів. за шляхів по яких різні рівні OSI стека взаємодіють між собою. Бездротові системи особливо сприйнятливі до DDoS атак. Найчастіше вживаними способами нападу на канальний рівень є керування рознесеними антенами. Інший найчастішою проблемою на канальному рівні бездротових мереж є спуфінг точок доступу, у тому числі з автентифікацією WEP. Сторона клієнта

зазвичай налаштовується таким чином, щоб зв'язуватися з точкою доступу з найбільш сильним сигналом, у свою чергу, атакуючий може підробити SSID точки доступу та клієнти підключатися до неї автоматично.

Також найбільш часто зустрічаються атаками є напади порушення трьох головних аспектів інформаційної безпеки – атаки на конфіденційність, цілісність та доступність.

Атаки на конфіденційність спрямовані на перехоплення особистої інформації, що передається бездротовою мережею у відкритому або зашифрованому вигляді, за допомогою 802.11 або протоколів верхнього рівня. Атаки на недоторканність (на цілісність). Цей вид атак посилає фрейми хибного контролю, управління або містять дані провокують збої на стороні одержувача, або застосовуються для полегшення проведення іншого виду атак. Атаки на автентифікацію здійснюються з метою крадіжки особистих даних, а також повноважень для подальшого доступу до інших сервісів та приватних мереж.

Провівши аналіз існуючих методів виявлення атак у бездротових мережах можна відзначити, що найактуальнішими засобами детектування є системи виявлення атак. Однак, в даний час час у зв'язку з широкими можливостями методів інтелектуального аналізу даних, проблему детектування щодо наявності ознак атаки можна вирішити, використовуючи ці методи. Через те, що системи виявлення бездротових атак молодих видів засобів захисту, функції та підходи до їх реалізації у досить серйозно відрізняються. Незважаючи на це, важливо відзначити такі завдання, які знаходять рішення за їх допомогою: створення карти бездротової мережі, облік мережевих пристроїв, діагностика пропускної спроможності бездротової мережі, контроль політик безпеки, детектування вразливостей конфігурації, виявлення та протидія атакам у бездротових мережах та інші.

Методи виявлення атак діляться на інтелектуальні та поведінкові. Поведінкові методи засновані на інформації про поведінку сканованої мережі, у свою чергу, в основі інтелектуальних методів закладена інформація про самі атаки. Моніторинг системи та подальший аналіз її стану на наявність аномалій може проводитись як статично у вигляді "знімка" середовища, так і динамічно в режимі реального часу. Інтелектуальні системи детектування атак містять у собі механізми виявлення популярних атак замість шаблону про стан мережі, однак, вони можуть не впоратися з їх модифікаціями, якщо заздалегідь вони не будуть додані в основу. Досить часто організація подібних систем вимагає впровадження нейронних мереж чи машинного навчання. Нейронні мережі використовують велика кількість різних алгоритмів навчання, перетворюючи вихідні дані на класифікацію аномалій мережі. Машинне навчання у свою черга будується на основі Байєсовських мереж зі стохастичним апаратом і дерев рішень.

Визначення вразливостей конфігурації бездротових мереж та протидія атакам у бездротових мережах є основами для забезпечення конфіденційності, цілісності та доступності інформації в мережах WLAN.

Список використаних джерел:

1. Беспроводные сети Wi-Fi / А.В. Пролетарский, И.В. Баскаков, Д.Н. Чирков и др.. М.: Интуит, 2007. - 216 с.
2. Щербаков А.К. Wi-Fi: все, что Вы хотели знать, но боялись спросить. — М.: Бук-Пресс, 2005. 239 с.
3. Інтернет-джерело: wi-fi. безпровідна мережа //URL: https://booksonline.com.ua/view.php?book=27964 / (дата звернення: 17.05.2022).
4. Інтернет-джерело: Механизм шифрования WEP // URL: http://wifi-zone.ucoz.ru/publ/l-l-0-33 (дата звернення: 18.05.2022).

Завадський Володимир В'ячеславович,
студент 5 курсу, групи БСДМ-53
Державного університету телекомунікацій, м. Київ
(095) 79-48-493, vovazavadskiy@gmail.com

ВАЖЛИВІСТЬ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У РОЗВИТКУ ДИСТАНЦІЙНОЇ ОСВІТИ

Анотація. *До цього часу було проведено чимало наукових досліджень щодо виробництва інноваційних технологій, широкого застосування в освіті та досягнення плідних результатів. Крім того, використовуються сучасні педагогічні технології у викладанні предметів усіх сфер освіти, готуються навчально-методичні посібники.*

Дистанційне навчання - це можливість навчання в індивідуальному режимі, незалежно від часу і місця, можливість навчання протягом усього життя. У всіх країнах світу зростає кількість студентів, які навчаються дистанційно, збільшується кількість університетів, які використовують ці технології в навчальному процесі; створено велику кількість міжнародних навчальних закладів. Сучасна освіта - це інтеграція змісту і технології навчання.

Серед технологічних засобів дистанційного навчання виділяють три основні групи: кейс-технології, TV-технології та мережеві технології.

При кейс-технології навчальні матеріали комплектуються в спеціальному комплекті (кейсах). Цей набір надсилається студенту для самостійного вивчення з періодичним зверненням до керівників факультету у створених для цих цілей Навчальних центрах. Зокрема, до цієї групи відноситься традиційна технологія дистанційного навчання. Вважається, що за достатньої мотивації студент здатний самостійно засвоїти і значний обсяг матеріалу з широкого кола дисциплін. ТБ-технологія, як випливає з її назви, заснована на використанні телелекцій.

До мережевим технологіям відносять Інтернет-технології і технології клієнт-сервер у локальних мережах. Як Інтернет-технології використовуються для надання Інтернету для навчання студентам навчально-методичними матеріалами, а також для взаємодії викладачів і студентів.

Інтернет - це зручне і доступне джерело різноманітної інформації. Це відкриває нові горизонти в інформаційному забезпеченні науки, забезпечуючи доступ до інформації в електронному вигляді, створюючи принципово нові ресурси, форми організації та спрямування науково-дослідницької та

навчальної діяльності. Проте необмежена кількість різноманітних за формою та змістом загальнодоступних мережевих ресурсів, які не завжди відповідають вимогам як студентів, так і викладачів. Виявляється, що в Інтернеті не вистачає якісних, добре структурованих і доступних ресурсів. Це питання стає все більш важливим у самостійному пошуку наукової та навчальної інформації.

У той же час технологія дистанційного онлайн-навчання має ряд істотних переваг перед іншими. Це дозволяє навчатися за індивідуальним графіком, постійно контактуючи з викладачем, іншими студентами та адміністрацією навчального центру. Підключення «багато до багатьох» є принциповою відмінністю Інтернет-технологій від інших технологій дистанційного навчання, що створює ефект «присутності» і породжується явищем під назвою «віртуальний університет».

Інтернет — майже ідеальний технічний інструмент для дистанційного навчання. Він може доставити студентам будь-який навчальний матеріал (підручник, відеолекції чи демонстрації експерименту) і навіть перевірити. Будь-яке навчання вимагає певної організаційної та інформаційної підтримки. Повинен мати такі складові: навчальний центр (школа) - організаційна структура дистанційної освіти; інформаційні ресурси - навчальні курси, довідкові, методичні та інші матеріали; засоби забезпечення технологій дистанційного навчання - організаційні, технічні та інші програмні засоби; вчителі, учні.

Основні функції, які необхідно виконати для організації та забезпечення належного функціонування системи дистанційної освіти: підтримка навчальних курсів; доставка навчального матеріалу учням; супровід довідкових матеріалів (бібліотека); консультування; контроль знань; організація спілкування студентів (колективне навчання).

Тому для дистанційного курсу необхідні чотири складові, які забезпечують навчальний процес: інформаційні ресурси; Засоби комунікації; тестування системи; системне адміністрування.

Забезпечити засіб комунікації як процес взаємодії з навчальним центром студента (зокрема, з викладачем) та з іншими учнями, що важливо.

Найважливіший компонент дистанційного курсу - інформаційні ресурси, на якому приділяється значна частина. Сьогодні матеріали, за якими складаються електронні навчальні курси, мають мультимедійний характер - текст, зображення, відео, комп'ютерна анімація, музика та голос. Тому одним із найважливіших завдань є організація різнорідної (мультимедійної) інформації у вигляді єдиної інформаційної системи, яка є навчальним курсом.

Використання як інструменту Інтернету та інших систем передачі даних «зближує» викладача та студентів, що знаходяться далеко один від одного, ближче до традиційної дистанційної освіти, у безпосередньому спілкуванні зі студентом-викладачем, викладачем з аудиторією, груповими семінарами, перевірений століттями. Тому дистанційне навчання часто називають формою навчання XXI століття.

Список використаних джерел:

1. У. Карімов, І. Касимов Матеріали міжнародної наукової конференції «Розширені інформаційні технології та наукові обчислення»

Кундик Валерія Олексіївна,
студент 4 курсу, групи САД-41
Державного університету телекомунікацій
(067) 638 87 44, lera.bonk@gmail.com
Науковий керівник: Бондарчук Андрій Петрович,
д.т.н., професор кафедри Інженерії програмного забезпечення
Державного університету телекомунікацій, м. Київ

ОПТИМІЗАЦІЯ ПРОЦЕСУ ОФОРМЛЕННЯ ТА РОБОТИ С СИЛАБУСАМИ В ДЕРЖАВНОМУ УНІВЕРСИТЕТІ ТЕЛЕКОМУНІКАЦІЙ

Постановка задачі. Завдяки впровадженню оптимізованої системи створення силабусів можна уникнути ключових проблем при створенні, редагуванні, узгодженні силабусів. Викладачеві та іншим особам (завідувач кафедри, група забезпечення освітньої програми, гарант освітньої програми та ін.) доводиться працювати з документами, що представлені в різних форматах, а також необхідністю контролювати в процесі складання силабусу контрольні числа навантаження та оцінювання студентів та відповідність вмісту силабусу пов’язаним документам. Також є проблема з дублюванням даних у вхідних документах для створення силабусу.

Мета дослідження. Метою дослідження є оптимізація процесу створення силабусу для зменшення кількості помилок, підвищення зручності та економії часу на його створення.

Результати дослідження. В результаті досліджень пропонується оптимізувати етапи пов'язані зі збереженням данних (на поточний момент дані зберігаются в форматі .docx, .pdf, базі даних розкладу) та об'єднати це все в єдину базу для можливості автоматизованого формування силабусу.

Також буде впроваджена оптимізація розрахунків даних силабусу, автоматизований контроль кількості годин, шо виділяются на окремі види занять, підвищення зручності формування силабусу.

Завдяки впровадженню інтерфейсних форм, зручий UI (випадаючі списки, check box, combo box та ін.) дозволить мінімізувати ручне заповнення документу та допоможе зменшити кількість помилок при складанні силабусу.

Для підвищення зручності редагування також пропонується формування силабусу в електронному вигляді, як елемента бази даних.

Висновки та перспективи. Завдяки оптимізації створення силабусів зменшено кількість помилок при заповненні документу, підвищено зручність заповнення та редагування, а також економії часу для заповнення силабусу.

Список використаних джерел:

1. ОНИЩЕНКО, В. В.; БОНДАРЧУК, А. П. Програмна інженерія: проблеми та перспективи. Зв'язок, 2015, 1: 10-13.

Зуб О. В.
Аспірант, група АКІ-123
Державного університету телекомунікацій
(068) 098 63 63
quartzov@gmail.com
Науковий керівник: Бондарчук Андрій Петрович,
доктор технічних наук, професор
Державного університету телекомунікацій, м. Київ

РОЛЬ СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В ЗАХИСТІ ІНФОРМАЦІЙНОГО ПРОСТОРУ

Синергетична взаємодія нанонаук, генної інженерії, інформаційних і новітніх гуманітарних технологій все більш радикально змінює людину, трансформуючи її людську природу, попереджують науковці. Неконтрольований вплив сучасного інформаційного середовища на свідомість фахівців, діяльність яких пов'язана із захистом кіберпростору України, вплив зовнішньої інформаційної експансії, внаслідок якої формується мережна залежність, можуть мати негативні наслідки в їх професійній справі. Сучасні можливості інформаційних технологій, що забезпечують доступність і великі обсяги інформації, з одного боку, і неусвідомлена спрямованість людини на опанування нею, з іншого, можуть сприяти формуванню поверхневого, безсистемного знання, коли втрачається зв'язок між отриманим знанням і майбутньою професійною діяльністю, загублюється цінність і значущість знання, пов'язаного із захистом інформаційного простору України.

Сучасні глобальні зміни, що супроводжуються підвищенням ризикогенності професійної діяльності, зумовлюють необхідність переосмислення значущості безпекової складової у підготовці фахівців до діяльності в непередбачуваних ситуаціях підвищеного ризику. Потреба у впровадженні в систему підготовки фахівців спецзв'язку і кібербезпеки, поряд із спеціальними знаннями, загальнотеоретичних знань про безпеку, з відповідною кореляцією світоглядних настанов обумовлена, також, посиленням проявів інформаційного тероризму в світі та Україні, зростанням масштабів гуманітарних і техногенних катастроф, соціальною девіацією. Спираючись на цілі, що визначені у Глобальній програмі дій з освіти в інтересах сталого розвитку, розробленої ЮНЕСКО, доцільно зробити висновок, що сучасна освіта, має втілювати випереджуючу підготовку людини до розв'язання кризових проблем суспільства, втілювати функцію формування антикризової поведінки особи.

Перелічені чинники надають підстави зробити висновок, що підготовка фахівців у сфері забезпечення кібербезпеки, має ґрунтуватися на системи базових професійних і гуманітарних знань, соціальних і професійних цінностей, моральних і правових засад, психологічних настанов, впровадження яких, має сприяти формуванню професійних і соціальних особистісних якостей, що відповідають сучасним вимогам професії і потребам часу. Результати підготовки фахівців мають відображуватись у відповідних компетентностях і здатностях.

Проведений аналіз вимагає орієнтуватись у підготовці фахівців, перш за все, на формування соціальних і професійних компетентностей, що відповідають вимогам професійної діяльності в сфері забезпечення спецзв'язку і кібербезпеки в умовах швидких технологічних змін, зростаючих ризиків і небезпек, які припускають спроможність фахівця приймати ефективні, відповідальні професійні і управлінські рішення в непередбачуваних умовах зростання ризику, враховуючи їх можливі соціальні наслідки. Згідно з окресленими компетентностями у контексті адаптації до безпекових потреб, важливим завданням підготовки фахівців є формування таких здатностей як комплексна (професійна, інтелектуальна, моральна, психологічна) готовність фахівця до професійній діяльності в умовах зростаючого ризику, воєнних, техногенних і гуманітарних загроз; прогнозування, попередження і подолання імовірних небезпек у професійній, службовій діяльності; здійснення самостійного, адекватного і відповідального вибору у прийнятті рішення в критичних професійних ситуаціях; критична оцінка і врахування небезпечних наслідків власної професійної діяльності й прийнятих рішень; самостійний пошук і відпрацювання наукових джерел для систематичного оновлення власних знань з метою загальнотеоретичного і професійного самовдосконалення. Врахування сучасних вимог до вищої освіти і внесення відповідних змін у програми навчальних дисциплін, як спеціального, так і гуманітарного профілю, є важливою умовою підвищення якості підготовки фахівців спецзв'язку і кібербезпеки.

Отже можна зробити висновок що розвиток інфокомуніційних систем і технологій у сучасному глобалізованому і небезпечному світі потребує впровадження у систему підготовки фахівців спецзв'язку і кібербезпеки, поряд із професійними знаннями, відповідної складової системи безпекових знань, превентивного мислення, антикризової поведінки, відповідальності за можливі наслідки прийнятих рішень, ціннісних орієнтацій і здатностей, що мають сприяти успішному виконанню професійних завдань в складних умовах підвищеного ризику. професійної діяльності.

Список використаних джерел:

1. ФУРАШЕВ, В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*, 2012, 2: 162-169.
2. ВАЛЮШКО, І. О. Кібербезпека України: наукові та практичні виміри сучасності. *Вісник НТУУ" КПІ" Політологія. Соціологія. Право*, 2016, 3/4 (31/32): 117-124.

Зарицька О.В.
студентка
Державний університет телекомунікацій
al.zariczckya@gmail.com
Науковий керівник – Варфоломеєва О.Г.
к.т.н., доцент кафедри Телекомунікаційних систем та мереж
Державний університет телекомунікацій

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ МЕРЕЖЕВОГО СЕРВІСУ ЗАСОБАМИ SDN

Анотація. *Розглядається проблема забезпечення якості мережевих сервісів. Можливість забезпечення якості мережевих сервісів засобами, які надають мережі SDN*

Як показують історія і практика використання комп'ютерних мереж, якість мережевого сервісу, яким хочуть володіти користувачі, завжди перевищує можливості наявної мережевої інфраструктури. Більш того, розрив між сукупністю вимог призначених для користувача додатків і доступною продуктивністю мережі продовжує збільшуватися [1]. Як наслідок, мережеві додатки змушені працювати в умовах постійної конкуренції за виділені на їх обробку ресурси мережі: пропускну здатність каналів передачі даних, процесорний час і обсяг буферів на мережевих пристроях.

Таким чином, проблема пошуку справедливого і в той же час ефективного розподілу доступних ресурсів між додатками є однією з найбільш фундаментальних проблем комп'ютерних мереж.

За роки дослідження означеної проблеми розроблено безліч різнопланових підходів до її вирішення як з боку додатків, так і з боку мережевої інфраструктури. Прикладами подібних підходів є адаптація і пріоритезація призначеного для користувача трафіку, динамічна маршрутизація, резервування ресурсів. Причому кожен з цих підходів дозволяє охопити лише частину вихідної задачі.

Таким чином, жоден з існуючих механізмів управління якістю сервісу не дає комплексного вирішення проблеми. Композиція ж відразу декількох засобів часто неефективна і не завжди можлива без їх модифікації. Наприклад, поєднання резервування ресурсів і маршрутизації потоків вимагає, щоб остання вважала зарезервовані ресурси зайнятими. Крім того, багато хто з існуючих методів висувають додаткові вимоги до функціональних можливостей і характеристикам ефективності мережевих пристроїв, які і без того мають обробляти мільйони пакетів щомиті. Наприклад, резервування ресурсів і маршрутизація потоків припускають, що кожний мережевий пристрій зберігає інформацію по всіх оброблюваних їм потоках і зіставляють з нею кожен пакет, який потрапляє в мережу [2].

Додавання такої логіки до сучасного комутаційного обладнання вимагає його істотного ускладнення і відповідного збільшення його вартості. Тому постачальники мережевих послуг часто змушені відмовлятися від просунутого управління якістю сервісу на користь більш низької вартості мережевої

інфраструктури.

У магістерській роботі пропонується використовувати для вирішення проблеми концепцію SDN (oftware-defined networking), в основу якої закладені принципи централізованого управління мережевими ресурсами і незалежної комутації потоків трафіку [3].

Іншими словами, в мережах SDN автоматично виконуються ті самі «незручні» вимоги, які перешкоджали масштабного впровадження існуючих методів управління якістю мережевого сервісу. Успішний розвиток даної технології роблять актуальними завдання адаптації відомих підходів до управління якістю сервісу до роботи в новому для них середовищі, а також завдання розробки нового комплексного механізму управління, що охоплює відразу кілька аспектів даної проблеми.

Методи оцінки різних параметрів якості сервісу і, в тому числі, затримки передачі пакетів можуть суттєво відрізнятися в залежності від пристрою мережі. У роботі наводиться аналіз найбільш важливих методів забезпечення якості сервісу, а також вимог, які ці методи пред'являють до пристрою і принципам функціонування мережевої інфраструктури. Розглянуто варіанти застосування SDN для підвищення якості мережевого сервісу.

Список використаних джерел:

1. Cisco Systems I. The Zettabyte Era: Trends and Analysis: white paper. — June 10, 2014.

2. Pana F., Put F. A Survey on the Evolution of RSVP // Communications Surveys & Tutorials. — 2013. — Vol. 15, no. 4. — Pp. 1859–1887.

3. Open Networking Foundation Software-Defined Networking: The New Norm for Networks: White paper. — 2012.

Леньо В. Я.
студент 4 курсу, групи ПД-41
Державного університету телекомунікацій
(099)2355413
wladlegno@gmail.com
Науковий керівник: Дібрівний О.А.,
доктор філософії, викладач кафедри Інженерії програмного забезпечення
Державного університету телекомунікацій, м. Київ

ЗАСОБИ ДЛЯ СТВОРЕННЯ 2D-ПЛАТФОРМЕРІВ

Задача - дослідження наявних інструментів та методів, що дозволяють створювати ігри жанру платформер. Метою є аналіз таких засобів.

Ігровий рушій - програма, що надає платформу для створення ігор, себто має функціонал, що спрощує керування проектом розробки гри.

Найрозповсюдженішим та найсучаснішим двигуном для побудови ігор у жанрі платформер можна вважати Unity.

Прикладами розроблених на Unity нових ігор у цьому жанрі можна вважати "Cuphead", "Ori and the Blind Forest", "RimWorld" та "Hollow Knight".

У 2005 році з'явився Unity, котрий задумувався для полегшення процесу

створення ігор на Mac OS X. Проте проект розвивався і наразі він підтримує усі найпопулярніші платформи та дозволяє розробляти 2D та 3D проекти різних жанрів.

Unity спрощує створення 2D сцен, керування камерою, персонажем та фізикою світу. Також прискорює процес створення користувацького інтерфейсу та використання графічних елементів у грі. Окрім того, один із найбільших плюсів Unity - його багатоплатформенність: гру потім легко адаптувати для будь-якої операційної системи, будь то настільні: Windows, OS X, Linux - мобільні: iOS, Android - або веб-простір.

Окрім того, функціонал Unity розширюється за рахунок плагінів - коду, котрий створено окремо від рушія, проте який можна підключити для збільшення або покращення наявного функціоналу. Найкориснішими плагінами для створення 2D-платформера можна назвати Cinemachine та Bolt.

Cinemachine - безкоштовний модуль до Unity, розроблений командою цього рушія. Цей проект дає змогу створювати якісні камери з уживанням мінімальної кількості коду. Набір інструментів не має залежносте, працює прямо після встановлення та з мінімальними налаштуваннями зі сторони розробника.

Bolt - безкоштовне доповнення для Unity, котре розроблене командою цього рушія. Дозволяє створювати логіку поведінки за допомогою візуального скриптування, тобто створення логіки гри та механік без написання коду, а використовуючи будівні блоки та їх реляції. Комфортний для швидкої розробки певних шаблонів та подальшого їх використання в інших частинах проекту.

Отже було проаналізовано різні засоби розробки проектів жанру 2D-платформер та їх особливості, що можуть у подальшому бути використані для створення власної гри.

Список використаних джерел:

1. Офіційний сайт рушія Unity [Електронний ресурс]: [Веб–сайт]. – електронні дані. – Режим доступу: https://docs.unity3d.com
2. Офіційний сторінка розширення для Unity Cinemachine [Електронний ресурс]:[Веб–сайт]–електронні дані.– Режим доступу: https://unity.com/unity/features/editor/art-and-design/cinemachine
3. Офіційний сторінка розширення для Unity Bolt [Електронний ресурс]: [Веб–сайт]. – електронні дані. – Режим доступу: https://assetstore.unity.com/packages/tools/visual-scripting/bolt-163802

Леньо В. Я.
студент 4 курсу, групи ПД-41
Державного університету телекомунікацій
(099)2355413
wladlegno@gmail.com
Науковий керівник: Дібрівний О.А.,
доктор філософії, викладач кафедри Інженерії програмного забезпечення
Державного університету телекомунікацій, м. Київ

ПЛАТФОРМЕРИ ЯК ЯВИЩЕ І ЇХ СУТНІСТЬ

Суть ігор жанру платформер полягає в маневруванні гравцем ігрового персонажу між платформ, звідки й назва, та інших перешкод за допомогою переміщень уверх, униз, уліво й управо, досягаючи таким чином цілі. Також одним із елементів гри можуть бути вороги.

Цей жанр зародився у 1980-му році з появою аркадної гри Space Panic, розробленої компанією Universal. Однак частіше першою грою-платформером називають Donkey Kong, розроблену у 1981-му році компанією Nintendo, тому що саме там з'являються визначні елементи жанру в цілому. Саме ця гра допомогла стати Nintendo вагомою компанією в інтернаціональній ігровій індустрії.

У 21-му столітті цей жанр утратив минулу популярність та займає малий процент ігрового ринку, проте цікаві ігри в даному жанрі так і далі випускаються та збирають прихильників

Вартими уваги іграми цього жанру є: “Mario”, “Ori and the Blind Forest”, “Limbo”, “Shovel Knight”, “Braid”, “Celeste” та інші.

Усі представники жанру мають у собі такі риси: фокус на процесі гри, а не на історії, просте керування. Також часто зустрічаються дуже динамічні ігри, або такі, де акцент зроблено на візуальній частині. Загалом жанр дуже варіативний та дає розробнику багато місця для креативу.

В основному ігри цього жанру невеличкі за розміром та довжиною в часі, не створюють сильного когнітивного навантаження та добре підходять для того, аби розслабитись. До того ж хороша візуальна та аудіо складова допомагають отримати насолоду від цифрової творчості.

Для створення платформеру потрібен ігровий рушій. Найпопулярнішими рішеннями на ринку наразі є CryEngine, Unreal Engine та Unity.

CryEngine був створений німецькою студією для розробки ігор Crytek і задумувався для внутрішнього використання. Рушій робить фокус на графічній складовій та дозволяє створювати ігрові проекти середнього та великого масштабів, а тому не підходить для створення платформерів.

Unreal Engine був розроблений у 1998 році для гри Unreal. Задумувався для шутерів на платформі PC, проте з часом його почали розробляти та використовувати для багатьох жанрів з орієнтиром на 3D-графіку, а також у фільмах. Рушій робить фокус на візуальній складовій, складних обчисленнях та реалістичності зображення, а тому не підходить для створення платформерів.

Unity був створений у 2005 році як рушій для розробки ігор на платформу Mac OS X, проте за історію свого розвитку навчився працювати з іншими

найпопулярнішими платформами. Ідеально підходить для створення ігор маленького та середнього розмірів та подальшого їх портування на інші платформи. Саме тому платформери зазвичай пишуться на Unity.

Актуальність гри для ринку України є майже повна відсутність конкурентів від вітчизняних компаній, проте потенційних гравців багато.

Отже ігри в жанрі платформер це такі ігри, котрі не несуть особливого когнітивного навантаження, візуально гарні, динамічні та швидкі у проходженні, а також наразі актуальні.

Список використаних джерел:

1. Стаття про ігри в жанрі платформер в енциклопедії Britannica [Електронний ресурс]: [Веб–сайт]. – електронні дані. – Режим доступу: https://www.britannica.com/topic/electronic-platform-game
2. Стаття про ігри в жанрі платформер Wikipedia [Електронний ресурс]: [Веб–сайт]. – електронні дані. – Режим доступу: https://en.wikipedia.org/wiki/Platform_game
3. Стаття про українські ігри-платформери [Електронний ресурс]: [Веб–сайт]. – електронні дані. – Режим доступу: https://leogaming.net/ua/site/news/maloizvestnye-kompyuternye-igry-ot-ukrainskih-razrabotchikov-1-nachalo
4. Типи платформ у іграх-платформерах [Електронний ресурс]: [Веб–сайт]. – електронні дані. – Режим доступу: https://www.idtech.com/blog/10-types-of-platforms-in-platform-video-games
5. Домашня сторінка рушія Unity [Електронний ресурс]: [Веб–сайт]. – електронні дані. – Режим доступу: https://unity.com/
6. Домашня сторінка рушія CryEngine [Електронний ресурс]: [Веб–сайт]. – електронні дані. – Режим доступу: https://www.cryengine.com/
7. Домашня сторінка рушія Unreal Engine [Електронний ресурс]: [Веб–сайт]. – електронні дані. – Режим доступу: https://www.unrealengine.com/

Івлєв Ростислав Володимирович
Студент 4 курсу, групи ПД-44
Державного університету телекомунікацій м. Київ
(093) 2415773
ivv.jpeg@gmail.com
Науковий керівник: Золотухіна О. А.,
кандидат технічних наук, доцент, доцент кафедри Інженерії програмного забезпечення
Державного університету телекомунікацій, м.Київ

ТЕХНОЛОГІЯ РОЗПОДІЛЕНОГО РЕЄСТРУ

Технологія розподіленого реєстру (Distributed Ledger Technology, DLT) – це технологія зберігання даних, де інформація спільно використовується та зберігається одночасно на різних пристроях, які знаходяться в різних місцях, утворюючи мережу, в якої нема єдиного контролю.

Кожна DLT мережі складається з вузлів, вони можуть бути різного типу та мати різню функціональність в залежності від розподіленого реєстру. Але наступні функцій обов’язково присутні хоча б у одного типу вузлів у кожній DLT мережі: реєстр, опрацювання запитів, механізм консенсусу.

Консенсусу в DLT мережах це механізм перевірки транзакцій, при якому позитивним рішення ґрунтується на відсутності заперечення. Найбільш відомі протоколи консенсусу – це Proof of Work (PoW) та Proof of Stake (PoS).

Реєстр зберігає всі транзакції, які були підтверджені та виконані. Перед тим як транзакція потрапляє до реєстру, вона повинна пройти наступні кроки [1]:

- Користувач створює транзакція відправляє її до мережі. Транзакція – це запит на будь яку маніпуляцію з реєстром аналогічно з SQL запитом, структура транзакції залежить від DLT мережі.
- Коли транзакція потрапляє до одного з вузлів та відповідає структурі, вона попадає в лог (мемпул) – це набір не підтверджених транзакції, який знаходиться на рівні вузла.
- Вузол випадково вибирає транзакції з свого лога та утворює запис-кандидат.
- Запис-кандидат підтверджується відповідно до протоколу консенсусу, який використовується у DLT мережі, після чого становиться підтвердженим записом-кандидатом, який поширюється між іншими вузлами.
- Коли інші вузли отримають поширений запис-кандидат, вони теж підтверджують його відповідно до протоколу консенсусу, після чого цей запис додається до журналу. Журнал – це копія реєстру, яка зберігається на вузлі. Дані в журналі можуть відрізнятися від вузла до вузла.
- Останній крок – це злиття синхронізованих журналів, які утворюють реєстр.

DLT мережі можна класифікувати за відкритістю контролю на такі типи [2]:

- Загальнодоступні – будь-який користувач може запустити власний вузол без потреби отримання дозволу від власника.
- Приватні – на відміну від загальнодоступних потребує отримання дозволу, що дозволяє обмежити доступ читання та здійснювання транзакцій.
- Гібридні – поєднують в собі попередні типи, що дозволяє власнику обмежити, які дані будуть публічні, а яка приватні.

Нема однієї стандартизованої реалізації технології розподіленого реєстру, через це існують концепції які переросли в типи, наприклад Tangle.

Список використаних джерел

1. Distributed ledger technology systems A Conceptual Framework [Електронний ресурс] / [M. Rauchs, A. Glidden, B. Gordon та ін.] // Cambridge Centre for Alternative Finance. – 2018. – Режим доступу до ресурсу: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf.

2. Distributed ledger technology overview, concepts, ecosystem [Електронний ресурс] // Telecommunication standardization sector OF ITU. – 2019. – Режим доступу до ресурсу: https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d12.

Шуляк Дарія Геннадіївна,
студентка 4 курсу, групи ТСД-41
Державного університету телекомунікацій
(097) 555 24 68
d.shuliak@gmail.com
Науковий керівник: Домрачева Катерина Олексіївна,
к.т.н., доцент кафедри Телекомунікаційних систем та мереж
Державного університету телекомунікацій, м. Київ

АНАЛІЗ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ІСНУЮЧИХ ПРОТОКОЛІВ AD-HOC МАРШРУТИЗАЦІЇ

Протоколи маршрутизації в мобільній мережі ad-hoc потребують різних підходів від існуючих Інтернет-протоколів, оскільки більшість з них були розроблені саме для підтримки маршрутизації в мережі з фіксованою структурою. Існує три типи протоколів ad-hoc маршрутизації, а саме проактивні або табличні (англ. proactive, table-driven), реактивні (англ. On-demand routing protocols), гібридні протоколи (англ. Hybrid protocols).

Проактивні протоколи, використовувалися одними з перших, як спосіб отримання маршрутизації в мобільних мережах ad-hoc. Ці протоколи забезпечують послідовний огляд мережі. Тобто, всі вузли цієї мережі використовують таблиці маршрутизації для зберігання інформації про розташування інших вузлів мережі. Цю інформацію вузли використовують для передачі даних один з одним в цій мережі. Щоб забезпечити актуальність таблиць маршрутизації, кожен вузол оновлює свої таблиці маршрутизації та дані про розташування інших вузлів-учасників у реальному часі. Одними з популярних протоколів цього типу для мобільних мереж ad-hoc є протокол векторної маршрутизації на відстані послідовності призначення (DSDV), протокол бездротової маршрутизації (WRP) і маршрутизація комутатора шлюзу кластера (CGSR).

Проактивні протоколи не можуть вважатися повністю ефективним рішенням для маршрутизації для мобільної мережі ad-hoc. Тому що наявність високої мобільності, великих таблиць маршрутизації спричиняють знижується пропускної спроможності та через мобільність, вимагають енерговитрат заряду акумулятора і тому час автономної роботи вузлів зменшується. До того ж постійні оновлення можуть створити непотрібні витрати на мережу.

Другим типом протоколів маршрутизації для мобільних мереж ad-hoc є реактивні протоколи. У цих протоколах, якщо вихідний вузол вимагає маршрут до місця призначення, а він не має інформації про це, то ініціює процес виявлення маршруту, способом проходження крізь всі вузли від одного до іншого, поки не досягне пункту призначення або проміжного вузла, який має маршрут до пункту призначення. Обов'язком вузла-одержувача є відповідь на запит вихідного вузла про можливий маршрут до пункту призначення. Після встановлення маршруту вузол джерела використовує його для передачі даних до вузла призначення. Деякі з найбільш відомих протоколів на вимогу - це тимчасова векторна маршрутизація за запитом (AODV), динамічна вихідна маршрутизація (DSR) і тимчасовий упорядкований алгоритм маршрутизації (TORA).

Хоча ці протоколи відрізняються від протоколів першого типу зберіганням відомої раніше інформації про маршрут і тим, яким саме чином використовують встановлені дані маршруту, та все ж у мережі з багатьма вузлами-учасниками ми знову ж таки можемо страждати від тих самих проблем, які ми проаналізували в протоколах, керованих таблицею. Тому цей тип протоколі також може вважатися не ефективним.

Існують також гібридні протоколи, які поєднують в собі переваги обох методів поширення маршрутної інформації. Прикладом гібридного протоколу є протокол зонової маршрутизації (ZRP, R-зоновий та ін.). Дані протоколи, не потребують так багато обчислювальних ресурсів та займають меншу частину смуги пропускання мережі, тому що вони поширюють тільки інформацію про зміни, а не всю таблицю маршрутизації, що особливо важливо для великих мереж.

Третій тип вважається найбільш ефективним, так як поєднує найкраще двох попередніх типів.

Список використаних джерел

1. Corson, S. & Macker, J. (1999) “Mobile Ad hoc Networking (MANET):Routing Protocol Performance Issues and Evaluation Considerations”, IETF rfc2501
2.Perkins, C. Belding-Royer, E. & Das, S. (2003) “Ad Hoc On-Demand Distance Vector (AODV) Routing”, IETF rfc3561.
3. Krishna, G. (2006) “Routing Protocols in Mobile Ad-hoc Networks”, Master’s Thesis in Computer Science, Umea University.
4. P. Basu, N. Khan and T. D. C. Little, "A mobility based metric for clustering in mobile ad hoc networks", Int. Distributed Computing Systems Workshop, pp. 413-418, 2001.

Панібратов Андрій Іванович
Студент 4 курсу, групи ПД-41
Державного Університету Телекомунікацій
(095) 522 92 73
andrewpan31@gmail.com
Науковий керівник: Золотухіна Оксана Анатолієвна,
к.т.н., доцент кафедри Системного аналізу
Державного університету телекомунікацій, м. Київ

ОГЛЯД ТА АНАЛІЗ ІНТЕРФЕЙСУ ДОДАТКІВ ДЛЯ АВТОМАТИЗАЦІЇ ОБЛІКУ КОМУНАЛЬНИХ ПОСЛУГ

Постановка задачі: огляд та аналіз додатків для автоматизації обліку комунальних послуг, що вже існують на ринку.

Мета: отримання кращого розуміння що до створення зручного та ефективного інтерфейсу для додатку по автоматизації обліку комунальних послуг.

Результати дослідження: Створення зручного інтерфейсу має особливо важливе значення, адже саме інтерфейс програми визначає наскільки легко

користувач зможе використовувати дане програмне забезпечення.. Головні складові успішного інтерфейсу можна описати у декількох пунктах [1]:

1)Зручність — це якість, що визначає, наскільки простим у використанні є інтерфейс.

2)Легкість опанування (Learnability) — тобто те, наскільки легко ваші користувачі можуть виконувати базові завдання під час першої взаємодії з продуктом.

3)Ефективність (Efficiency) — тобто те, наскільки швидко користувач виконує в інтерфейсі задачі, опанувавши його.

4)Запам'ятовуваність (Memorability) — це те, наскільки просто користувачеві буде згадати, як працювати з інтерфейсом, після тривалої перерви.

5)Робота з помилками (Errors) — як часто користувачі припускаються помилок, наскільки серйозними є ці помилки, і наскільки легко користувачі можуть з ними впоратись.

6)Задоволеність (Satisfaction) — наскільки приємним для користувача є дизайн продукту.

Дружній до користувача інтерфейс дозволить користувачу використовувати програмне забезпечення максимально ефективно, а отже розуміння процесу створення зручного інтерфейсу є надзвичайно важливим для повної реалізації потенціалу додатку. Розглянемо інтерфес декількох додатків та веб-ресурсі що вже існують на ринку.

Один з них – веб-сайт Yasno, що містить у собі функціонал для керування комунальними платіжками що стосуються електроенергії [2]. Сам сайт виводить свій головний функціонал на головне меню, полегшуючи роботу для користувача та роблячи користування сайтом набагато зручнішим. Це також дозволяє досягнути легкості в опануванні та ефективності у майбутньому, адже таке розташування функціоналу допомагає людині опанувати сайт без особливих складностей. Невелика кількість додаткових меню дозволяє повернувшемуся користувачу з легкістю повернути свої навички у роботі із сайтом і, як додатковий ефект, зменшує кількість можливих помилок. Варто зауважити, що дизайн, попри свою мінімалістичність, поєднує у собі приємні кольори, що, у свою чергу, піднімає задоволеність користувача. З усього перечисленого можна дійти до висновку, що веб-сайт Yasno робить усе можливе для отримання зручного та дружнього до користувача інтерфейсу.

На відміну від вузько спеціалізованого Yasno, ЦКС (Центр Комунальних Послуг) надає широкий вибір можливих послуг, який просто неможливо вмістити у одному меню [3]. Тут використовується інший підхід – усі послуги та дані розміщені у своїх власних додаткових вкладинках та вікнах, дозволяючи не втрачати зручність у користуванні такою великою кількістю послуг. Така велика кількість даних створює складнощі при опануванні чи поверненні до роботи, і підхід ЦКС до користувацького інтерфейсу не допомагає користувачу, адже деякі послуги можуть бути поєднані у одному вікні. Проте варто зауважити,що після успішного опанування така система є досить ефективною, економлячи багато часу для користувача. ЦКС також використовує дуже візуально приємний дизайн інтерфейсу, що базується на легко зрозумілих для

користувача візуальних елементах і, таким чином, допомагають користувачеві опанувати веб-додаток.

На останок розглянемо мобільний додаток “Комуналка” [4]. На відміну веб-додатків, мобільний додаток може повністю сконцентруватися на перевагах що надає touch-screen. Додаток має мінімалістичний стиль і намагається розділити свій невеликий функціонал на якомога більшу кількість під-меню. На телефоні такий метод доволі зручний та надає користувачу просте розуміння про дані, які той переглядає у той чи інший момент. Хоча користувачу усе ще потрібно пройти період ознайомлення та адаптації до додатку, Комуналка, завдяки розділенню інформації на невеликі підгрупи, досягає високого рівня у своїй ефективності при роботі. Дизайн додатку використовує темні кольори, що досить важливо для сприйняття інформації на мобільному телефоні без подразнення очей.

Висновки: Огляд інтерфейсу додатків для автоматизації сплати та обліку комунальних послуг громадян показує, що зазвичай додатки адаптують свій інтерфейс під платформу на якій знаходяться, а також під свій функціонал. Це значно підвищує задоволеність користувача та ефективність роботи з самим додатком.

Список використаних джерел

1) Головне про зручність в інтерфейсах [Електронний ресурс] // Creative Practices. – 2021. – Режим доступу до ресурсу: https://cases.media/article/golovne-pro-zruchnist-v-interfeisakh.\

2) Yasno [Електронний ресурс] – Режим доступу до ресурсу: https://yasno.com.ua/.

3) ЦКС [Електронний ресурс] – Режим доступу до ресурсу: https://cks.com.ua/cabinet/objects/.

4) Сайт “Центр Комунальних Послуг”: мобільний додаток”Комуналка”. [Електронний ресурс] – Режим доступу: Комуналка | ЦКС (cks.com.ua) 18.04.2022

Івлєв Ростислав Володимирович
Студент 4 курсу, групи ПД-44
Державного університету телекомунікацій м. Київ
(093) 2415773
ivv.jpeg@gmail.com
Науковий керівник: Золотухіна О. А.,
кандидат технічних наук, доцент, доцент кафедри Інженерії програмного забезпечення
Державного університету телекомунікацій, м.Київ

ТЕХНОЛОГІЯ РОЗПОДІЛЕНОГО РЕЄСТРУ

Мета роботи - ознайомити слухачів з технологією розподіленого реєстру.

Технологія розподіленого реєстру (Distributed Ledger Technology, DLT) – це технологія зберігання даних, де інформація спільно використовується та зберігається одночасно на різних пристроях, які знаходяться в різних місцях, утворювачі мережу, в якої нема єдиного контролю.

Кожна DLT мережа складається з вузлів, вони можуть бути різного типу та мати різню функціональність в залежності від розподіленого реєстру. Але наступні функцій обов’язково присутні хоча б у одного типу вузлів у кожній

DLT мережі: реєстр, опрацювання запитів, механізм консенсусу.

Консенсус в DLT мережах це механізм перевірки транзакцій, при якому позитивне рішення ґрунтується на відсутності заперечення. Найбільш відомі протоколи консенсусу це Proof of Work (PoW) та Proof of Stake (PoS).

Реєстр -це база даних яка зберігає всі транзакції які були підтверджені та виконані. Перед тим як транзакція потрапляє до реєстру вона повинна пройти наступні кроки [1]:

- Користувач створює транзакція відправляє її до мережі. Транзакція – це запит на будь яку маніпуляцію з реєстром, структура транзакції залежить від DLT мережі.
- Коли транзакція потрапляє до одного з вузлів та відповідає структурі вона попадає в лог (мемпул) – це набір не підтверджених транзакції який знаходиться на рівні вузла.
- Вузол випадково вибирає транзакції з свого лога та утворює запис кандидат.
- Запис кандидат підтверджується відповідно до протоколу консенсусу який використовується у DLT мережі, після чого становиться підтвердженою записом кандидатом яка поширюється між іншими вузлами.
- Коли інші вузли отримають поширений запис кандидат, вони теж підтверджують його відповідно до протоколу консенсусу, після чого цей запис додається до журналу. Журнал – це копія реєстру яка зберігається в вузлі. Дані в журналі можуть відрізнятися від вузла до вузла.
- Останній крок це злиття синхронізованих журналів які утворюють реєстр.

DLT мережі можна класифікувати за відкритістю контролю на такі типи [2]:

- Загальнодоступні - любий користувач може запустити власний вузол без потреби отримання дозволу від власника.
- Приватні - відміно від загальнодоступного потребує отримання дозволу, що дозволяє обмежити доступ к читанню та здійснюванню транзакцій.
- Гібридні - поєднують в собі особливості попередніх типів що дозволяє власнику обмежити які дані будуть публічні, а які приватні.

Нема однієї стандартизованої реалізації технології розподіленого реєстру через це існують концепції які переросли в типи, наприклад Tangle.

Список використаних джерел

1. DISTRIBUTED LEDGER TECHNOLOGY SYSTEMS A Conceptual Framework [Електронний ресурс] / [M. Rauchs, A. Glidden, B. Gordon та ін.] // Cambridge Centre for Alternative Finance. – 2018. – Режим доступу до ресурсу: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf.
2. Distributed ledger technology overview, concepts, ecosystem [Електронний ресурс] // TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU. – 2019. – Режим доступу до ресурсу: https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d12.pdf.

Тонкошкур Антон Юрійович
студент
Навчально-науковий інститут Телекомунікацій
Державний університет телекомунікацій,м. Київ

ОСОБЛИВОСТІ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ У ПРОМИСЛОВОМУ КОМПЛЕКСІ

У даній статті розглянуті загальні ознаки бездротових сенсорних мереж(БСМ). Тільки після ознайомлення із цим інформаційним витягом стає можливим виокремлення БСМ, як першочергової системи для моніторингу промислового комплексу. Наявність практичної, технічно доповненої системи полегшує збір аналітичного матеріалу для подальшого коректного керівництва підприємством.

Бездротова сенсорна мережа (БСМ) - це розподілена мережа, що самоорганізується та складається із безлічі сенсорів і виконуючих пристроїв, об'єднаних між собою за допомогою радіосигналу. Область покриття подібної мережі може становить від декількох метрів до декількох кілометрів за рахунок низки технічних характеристик елементів. Якщо брати до уваги нинішні реалії, то БСМ є фактично основою для побудови інтелектуальних систем моніторингу, які вже застосовуються на підприємствах(система охорони праці на шкідливому виробництві, система моніторингу параметрів машин і механізмів).

Апаратна частина вузла БСМ може бути поділена на наступні підсистеми: - комунікаційна підсистема(забезпечує бездротовий зв’язок з іншими вузлами в сенсорної мережі і містить радіо приймач); -обчислювальна підсистема(забезпечує обробку даних і функціональність вузла і складається з мікроконтролера MCU, до складу якого входять процесор,оперативна SRAM, незалежна EEPROM і флешпамять, аналого-цифровий перетворювач, таймер, порти введення/виводу); - сенсорна підсистема(забезпечує з’єднання сенсорного бездротового вузла із зовнішнім світом, до складу якої можуть входити аналогові і цифрові сенсори); - підсистема електроживлення.

Також ми маємо брати до уваги відмінність вузлів БСМ за архітектурою, а саме: координатор; маршрутизатор; кінцевий вузол.

Координатор – здійснює глобальну координацію, організацію та установку параметрів мережі, найбільш складний пристрій БСМ - вимагає найбільший об'єм пам'яті і найбільш потужне джерело живлення. В одній мережі повинен бути присутнім тільки один координатор. З координатора здійснюється вихід в зовнішню мережу. Часто координатор називають базовою станцією (БС).

Маршрутизатор - приймає, буферизує і передає дані від інших вузлів БСМ, а також визначає напрямок передачі.

Кінцевий пристрій (сенсорний вузол) – виконує тільки збір інформації та управління віддаленим об'єктом і не здійснює ретрансляцію даних.

До найбільш поширених топологій, які використовуються в БСМ належать: топологія зірка; деревоподібна топологія; коміркова топологія.

Топологія зірка – це мережева топологія, в якій всі вузли безпосередньо з’єднуються з основним вузлом – шлюзом. Цей вузол є лише одним, він може

відправляти або приймати повідомлення іншим вузлам. В топології зірка вузли, які не є шлюзом не можуть обмінюватися повідомленнями один з одним, лише з єдиним шлюзом. Це забезпечує обмін даними з низьким рівнем затримки між вузлами і шлюзом. Перевагою є те, що звичайні вузли потребують мінімального споживання енергії для роботи, бо основним їх завданням є лише передача інформації на головний вузол – шлюз. Розміри мережі залежать від кількості вузлів, які підключаються до шлюза.

Деревоподібну топологію також називають каскадною зірковою топологією. В топології дерева кожен вузол з'єднується з вузлом вище по топології, доходячи до кінцевого єдиного вузла – шлюза. Головною перевагою деревоподібної топології є те, що вона може бути легко масштабована, а також легким є виявлення можливих несправностей в ній.

Коміркова топологія дозволяє вузлам передавати дані до інших вузлів, які знаходяться в діапазоні радіопередачі. Якщо вузол хоче передати дані іншому вузлу, який знаходиться поза діапазоном можливої радіопередачі, йому потрібен проміжний вузол для пересилки повідомлення на потрібний. Перевагою такої топології є можливість простої ізоляції і виявлення несправностей мережі.

Роль телекомунікацій на підприємстві є фундаментальною. Завдяки продуманому, стратегічному та спільному підході, вони можуть бути ще більш ефективним засобом забезпечення своєчасного реагування або попередження виникнення НС на підприємстві. Розглянуті технологічні риси БСМ та аналіз проблематики їх створення в зоні де трапилася аварія, спонукають розглянути основні бездротові технології, які використовуються для передачі даних в сенсорних мережах, а також топології бездротових мереж. За для реалізації власної експериментальної БСМ з інфокомунікаційними наземними вузлами, а також подальшого освітлення шляхів модернізації сенсорних мереж.

Основними підсумками даної роботи є наступні: БСМ завдяки ряду переваг, таких як швидкість розгортання, тривалий час автономної роботи в суворих умовах експлуатації, здатність продовжувати роботу після виходу з ладу одного чи декількох вузлів, можливість масштабування, можуть ідеально підійти для використання в зоні, де потенційно може статися аварія; попри те, що існує багато бездротових технологій, які можуть використовуватися в сенсорних мережах, найбільш доцільно використовувати технологію Wi-Fi через ряд переваг, серед яких висока пропускна спроможність і система захисту інформації, що передається; реалізовано експериментальну сенсорну мережу з інфокомунікаційними наземними вузлами.

Список використаних джерел

1. Network topology[Електронний ресурс] / Режим доступу: https://en.wikipedia.org/wiki/Network_topology
2. Edgar H. Callaway. Wireless Sensor Networks - CRC Press, 2003, 360с.
3. Бездротова сенсорна мережа [Електронний ресурс] / Режим доступу: https://uk.wikipedia.org/wiki/ Бездротова_сенсорна_мережа

Шульженко Кирило Васильович
студент 5 курсу, групи КНЗ-51
Державного університету телекомунікацій
0930598230
Зінченко Ольга Валеріївна
д.т.н., завідувач кафедри Штучного інтелекту,
Державного університету телекомунікацій
Фесенко Максим Анатолійович
к.т.н, доцент кафедри Штучного інтелекту,
Державного університету телекомунікацій

РОЗРОБЛЕННЯ МОДУЛЯ ДЛЯ АНАЛІЗУ КЛІМАТ-КОНТРОЛЮ В ПРИМІЩЕННЯХ НА ОСНОВІ АПАРАТНОЇ ПЛАТФОРМИ ARDUINO

Одним із важливих питань сьогоднішнього періоду в Україні та у світі в цілому є впровадження заходів щодо енергозбереження.

Типовим рішенням з енергозбереження є регулювання температури теплоносія від теплогенеруючих установок залежно від температури навколишнього повітря. Цей метод досить ефективний в умовах житлової забудови, проте не підходить для керування температурою адміністративних будівель та приміщень. Істотними особливостями подібних будівель є:

– різнорідність приміщень за часом та кількістю співробітників та відвідувачів;

– різний набір та різні періоди включення приладів, пристроїв, засобів обчислювальної техніки.

У приміщеннях, де працюють засоби обчислювальної техніки та розташовується велика кількість людей, температура починає підвищуватися понад норму, тоді як у порожніх приміщеннях вона буде в нормі. Примусові хаотичні провітрювання приміщень, що нагріваються, не покращують ситуацію із забезпеченням енергоефективності будівлі.

Прикладом адміністративної будівлі, в якій є подібні проблеми, є приміщення та аудиторії у навчальних закладах. Лабораторні та аудиторні приміщення мають хвилеподібний ступінь заповнення та, як наслідок, клімат у цьому приміщенні регулюється шляхом постійних провітрювань (фактично виведення теплової енергії на вулицю).

Щоб не залежати від погодних умов та перепадів температур на вулиці та регулювати, а також підтримувати оптимальний клімат у приміщенні, можливо створити спеціалізовану систему обладнання для інтелектуального контролю та управління кліматом у приміщенні. До компонентів подібної системи можуть відноситися:

– автономний датчик температури та вологості у приміщенні;

– механічний терморегулятор з автоматичним керуванням або електронний терморегулятор;

– централізована система управління терморегуляторами.

Подібна система дозволить ефективно керувати витратою теплоносія в кожному приміщенні з урахуванням періодів додаткової теплогенерації

відвідувачами у приміщенні та/або включеними приладами та засобами обчислювальної техніки.

Розроблення автономного датчика температури та вологості є першим етапом побудови інтелектуальної системи керування кліматом у будівлі. Розташовані в різних частинах будівлі автономні датчики збирають відомості про стан навколишнього середовища і передають їх на сервер для запису в базу даних, необхідну для роботи керуючих елементів системи клімат-контролю.

Сучасний ринок нових технологій пропонує досить широкий асортимент засобів клімат-контролю. Проте більшість із них сильно спеціалізовані та вузькоспрямовані (наприклад, це засоби для контролю клімату у приміщеннях рослинних та тваринницьких виробництв, а також контролю стану кімнат зі спецобладнанням). Крім цього, до недоліків потрібно віднести полярно різні складові компонентів систем – вони або йдуть повним комплектом, який обов'язково необхідно купувати хоча б мінімальним набором і в якому недоцільно дорого і складно замінити один або кілька складових, або взагалі не є цілісною сукупністю.

Таким чином, стає доцільним створювати систему зі своїх відкритих компонентів, придатних до подальшого масштабування.

Як платформа для створення прототипу модулю для аналізу клімат-контролю у приміщенні було обрано відкритий мікроконтролер Arduino.

Arduino – апаратна обчислювальна платформа, основними компонентами якої є проста плата введення-виводу. Вона застосовується для створення електронних пристроїв з можливістю прийому сигналів від різних цифрових та аналогових датчиків, які можуть бути підключені до нього, та управління різними виконавчими пристроями. Проєкти пристроїв, що базуються на Arduino, можуть працювати самостійно або взаємодіяти з програмним забезпеченням на комп'ютері [1].

В роботі запропоновано схему модуля для контролю параметрів вологості та температури в приміщенні на базі мікроконтролерів ATMEGA8. Безпосередньо для контролю параметрів вологості та температури було обрано інтегральний датчик температури DHT22. Такий інтегральний діодний датчик температури є найсучаснішим, що швидко розвиваються та вбудовуються в мікросхеми і широко використовуються в електроніці [2]. Принцип роботи датчиків ґрунтується на залежності вольт-амперної характеристики напівпровідникового діода від температури. Датчик температури, вологості DHT22, як цифрового сигналу передає на контролер показники температури та вологості середовища, в якому він знаходиться.

У рамках поточного етапу виконання роботи вирішено:

– складання апаратної частини автономного датчика (контролер, датчики температури та вологості, програмний код);

– виконано перевірку коректності та повноти виміряних датчиком показань.

В рамках наступного періоду буде реалізовано:

– підключення до мікроконтролера модуля;

– налаштування взаємодії між контролером та сервером збору даних;

– створення бази даних для зберігання значень параметрів;

– оцінка економічної ефективності та доцільності подальшої реалізації проєкту в цілому.

Список використаних джерел:

1. Програмування Ардуїно URL: https://doc.arduino.ua/ru/prog/ (дата звернення 01.04.2022 р.).
2. Разработка автономного датчика температуры и влажности на основе аппаратной платформы Arduino URL: https://elar.urfu.ru/bitstream/10995/34902/1/tim_2015_77.pdf (дата звернення 01.04.2022 р.).

Журенко Ангеліна Олегівна
Студентка 5 курсу, групи КСДМ-51
Державного університету телекомунікацій
(096)5484396
a.zhurenko@students.dut.edu.ua
Науковий керівник: Боднарчук Андрій Петрович
д.т.н., професор кафедри Інженерії програмного забезпечення
Державного університету телекомунікацій, м.Київ

ОЦІНКА ЯКОСТІ ПОСЛУГ МЕРЕЖ IP

Розглянуто питання оцінки якості телекомунікаційних послуг у контексті їхньої конвергенції в рамках мереж наступного покоління. Обґрунтовано актуальність створення моделі параметрів якості послуг IP-мереж як основи NGN. Проаналізовано мережеві характеристики, властиві мережам IP та визначений найбільший вплив на якість надання послуг. Запропоновано модель, що структурує параметри якості послуг IP-мереж, представлені параметри оцінки якості послуг з погляду користувача, що дозволяють найповніше відобразити сприйняття якості послуг користувачем.

В даний час завдяки значному розвитку ринку інфокомунікаційних послуг відбувається інтенсивне впровадження нових технологій як в галузі інформатики, так і в галузі телекомунікацій, що, у свою чергу, сприяє стрімкому розвитку інфокомунікаційних мереж, зокрема мереж наступного покоління (NGN). Для NGN сьогодні характерні такі ознаки як великі розміри, складність, розвинені функціональні можливості [1].

З розвитком інфокомунікацій постійно зростають вимоги якості передачі інформації. Отже, збільшується потреба у виробленні сучасних методик оцінювання якості послуг та створення систем управління якістю. І якщо завдання оцінки та управління якістю послуг приймання/передачі мови (телефонія) добре опрацьовані та досліджені, а результати успішно застосовуються на практиці, то стосовно мультисервісних мереж, якими є мережі наступного покоління, аналогічні завдання ще не вирішені повною мірою. З проникненням інфокомунікаційних технологій у повсякденне життя безлічі людей, які мають різні переваги та вимоги, важливою є необхідність орієнтування на думку та потреби кінцевого користувача інфокомунікаційних

послуг.

Ще недавно мережі з комутацією каналів (телефонні мережі) і мережі з комутацією пакетів (IP (Internet Protocol)-мережі передачі) існували майже незалежно друг від друга і використовувалися різних цілей: телефонні мережі передачі голосової інформації, IP-сети - для передачі. Певною віхою в історії телекомунікацій та Інтернету є IP-телефонія, яка дозволила передавати "голос" поверх тих, що вже отримали значне поширення IP-мереж. На сьогоднішній день найбільш розвиненою технологією таких мереж є NGN, побудовані на базі протоколу IP [2], що забезпечує можливість надання конвергентних послуг: передачу голосу, зображення та даних по єдиній мережі, що обумовлено єдиною формою передачі інформації - поданням її у вигляді пакета.

На сьогоднішній день ведуться інтенсивні роботи зі створення нових точних, універсальних та простих у використанні методів визначення показників якості послуг, придатних для використання в мультисервісних мережах щодо існуючих та запропонованих для впровадження у майбутньому видів послуг. Існуючі моделі оцінювання якості послуг дозволяють оцінювати окремі параметри якості, але механізм комплексної оцінки не існує. NGN з властивою їм неоднорідністю, обумовленою різними мережами передачі даних (IP, ТфОП, мережі мобільного зв'язку), що входять до їх складу, ставлять завдання комплексної оцінки якості наданих послуг, яка повинна ґрунтуватися, в першу чергу, на оцінці якості послуг, що надаються кожною з мереж , що входять до її складу. У свою чергу, для оцінки якості послуг кожної конкретної мережі зв'язку необхідно створення моделі визначення параметрів якості послуг цієї мережі, що є важливим щодо IP-мереж, що становлять основу NGN.

В даний час існує трикутна модель визначення параметрів якості, розроблена ETSI для послуг мобільного зв'язку [3]. Модель комплексно описує та структурує параметри якості послуг зв'язку, визначаючи основні аспекти взаємодії користувача з мережею зв'язку та послугами. Подібний підхід до створення моделі параметрів якості є ефективним через простоту та наочність, що дозволяє його використання щодо визначення параметрів якості послуг інших мереж передачі даних, зокрема мереж IP.

Сучасною тенденцією багатьох постачальників послуг є зміщення акценту з удосконалення технічної складової послуг на безпосереднє задоволення запитів користувачів. Відповідно до такої тенденції запропонована в роботі модель визначення параметрів якості послуг, що надаються мережами IP [4], враховує характеристики користувача, ставлячи їх у відповідність технічним, мережевим характеристикам. Для суб'єктивної оцінки якості послуг в мережах IP використовуються метод оцінки MOS (середня оцінка думки) та метод одиниць рейтингу QR (Quality Rating), що описують якість у сприйнятті користувача (добре, погано, і т.д.) і ставлячи його у відповідність до значень технічних параметрів. Набір основних параметрів мережі, що впливають на якість передачі даних в мережах IP, описаний в Рекомендації Y.1540:

- продуктивність мережі;
- надійність мережі/мережевих елементів;
- Затримка доставки пакета (IPDT);
- варіація затримки пакета – джиттер (IPDV);

- Коефіцієнт втрати пакетів (IPLR);
- Коефіцієнт помилок пакетів (IPER).

Також виділяються параметри якості послуг, що визначають клієнт-орієнтованість моделі: доступ до послуги (надається оператором за бажанням абонента скористатися якоюсь послугою); повнота послуги (відбиває якість послуги безпосередньо для кінцевого користувача); безперервність послуги (характеризує умови завершення надання послуги); а також параметр, що впливає на якість будь-якої послуги - затримка доставки пакета (IPDT). Таким чином, пропонована модель враховує об'єктивні та суб'єктивні показники для комплексного опису параметрів якості послуг.

Запропонована модель має розподіл на рівні, що визначають основні аспекти взаємодії користувача з мережею зв'язку та послугою. Моделі параметрів якості послуг мереж IP мереж властива особливість - набір параметрів якості єдиний всім видів послуг, що пояснюється єдиною формою передачі у мережах IP (пакет). Відповідно до структури моделі, оцінка користувача може проводитися на двох рівнях.

- першому рівні – рівні доступу до мережі. Суб'єктивно користувач може оцінити швидкість встановлення з'єднання, чим коротше очікування, тим вища якість;

- третьому рівні – рівні послуг, що надаються мережею.

Таким чином, пропонована модель структурує мережеві параметри якості послуг, представляючи їх у зв'язку з параметрами користувача, що забезпечує можливість найбільш повної оцінки якості інфокомунікаційних послуг, що надаються мережами IP.

Список використаних джерел:

1. Salina, Jingming Li. Next Generation Networks: perspectives and potentials / Jingming Li Salina and Pascal Salina. John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England.
2. Internet Protocol, Version 6 (IPv6) Specification. (Электр.ресурс). Режим доступа: http://www.ietf.org/rfc/rfc2460.txt.
3. Тихвінський В.О., Терентьєв С.В. Управління та якість послуг у мережах GPRS/UMTS. - М.: Еко-Трендз, 2017. - 400 с.
4. Мурай А.В. Оцінка якості послуг мереж IP як бази NGN. XI-та Всеукраїнська науково-технічна конференція «Математичне моделювання та інформаційні технології» (ММІТ-2018). Тези доповідей. -Одеса: ОДАХ, 21-23 листопада 2018 р., С.126-127.

Алексіна Поліна Олегівна
Студентка 5 курсу, групи КСДМ-51
Державного університету телекомунікацій
(095)8329522
l.aleksina@students.dut.edu.ua
Науковий керівник: Боднарчук Андрій Петрович
д.т.н., професор кафедри Інженерії програмного забезпечення
Державного університету телекомунікацій, м.Київ

ПРОЕКТУВАННЯ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В ПРОЦЕСІ ВІДНОВЛЕННЯ І ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСНОГО ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

Однією з основних завдань під час створення складної системи є вибір її структури, що визначає внутрішню організацію та стійкі взаємозв'язки елементів системи. Завдання проектування структури тісно пов'язані із завданнями оптимізації функціонування систем та забезпечення її інформаційної безпеки. Структура вважається оптимальною, якщо загальна ефективність системи, що розробляється, максимальна.

У кожній інформаційній системі можна виділити найслабші місця з точки зору безпеки. На них необхідно звернути увагу насамперед. До таких місць, звичайно, належать сховища даних, адміністративна система, кабельна система, система доступу із зовнішніх мереж. Забезпечення захисту в системах відбувається за умов випадкового дії різних чинників, частина є систематизованою в стандартах, а частина заздалегідь невідомі. Оцінка ефективності систем захисту інформації (СЗІ) повинна обов'язково враховувати як об'єктивні обставини, так і ймовірнісні чинники, та її характеристики повинні мати імовірнісний характер. Особливу важливість на етапі розвитку інформаційних технологій (ІТ) має обґрунтування оптимальних значень показників ефективності та цільове призначення системи. Чим більш конкретно сформульована мета захисту інформації, детально з'ясовані ресурси, які залучаються для цього, а також визначено комплекс обмежень, тим більшою мірою очікується отримання бажаного результату. Якщо мета забезпечення інформаційної безпеки проста і принципово досягається, то виявляється досить порівняно нескладних за складом та структурою засобів захисту інформації.

Однак при розширенні кола проблем забезпечення інтегральної інформаційної безпеки зміст цільового призначення системи на формалізованому рівні матиме багатовимірний, векторний характер. При цьому значимість властивостей окремих елементів засобів захисту інформації знижується, а на перший план висуваються загальносистемні завдання - визначення оптимальної структури та режимів функціонування системи, організація взаємодії між її елементами, облік впливу зовнішнього середовища тощо. При цілеспрямованому об'єднанні елементів у систему остання буде мати специфічні властивості, спочатку не властиві жодній із її складових частин. При комплексному підході мають першорядне значення ті властивості елементів, які визначають взаємодію друг з другом і впливають на систему загалом [2].

Проектування, організація та застосування СЗІ ІС фактично пов'язане з невідомими подіями у майбутньому і тому завжди містять елементи

невизначеності..

Об'єктивною характеристикою якості СЗІ - ступенем її пристосованості до досягнення рівня безпеки, що вимагається, в умовах реальної дії випадкових факторів, може бути ймовірність, що характеризує ступінь можливостей конкретної СЗІ за заданого комплексу умов. Іншими словами – достовірність досягнення мети операції або достовірність виконання завдання ІС. Ця достовірність має бути встановлена в основу комплексу показників та критеріїв оцінки ефективності СЗІ. Під час синтезу системи виникає проблема вирішення задачі із багатокритеріальним показником. При цьому розглядаються показники ефективності, які призначені під час вирішення завдання порівняння різних структур СЗІ. Оцінка оптимального рівня гарантій безпеки певною мірою залежить від збитків, пов'язаних із помилкою у виборі конкретного значення показника ефективності. Для отримання чисельних оцінок ризику потрібно знати розподіл низки випадкових величин. Це певною мірою обмежує кількісне дослідження рівнів гарантій безпеки, що надаються СЗІ, але у багатьох практичних випадках такі оцінки можна отримати за допомогою імітаційного моделювання або за результатами активного аудиту СЗІ.

Список використаних джерел:

1. С.В. Толюпа Комплексний підхід оцінки ефективності систем захисту інформації в інфокомунікаційних мережах нового покоління / О.М. Власов, С.В. Толюпа // Наукові записки Українського науково-дослідного інституту зв'язку. наук.-вироб. зб. - 2011 - №3 (19). - С. 38-45.
2. Цвіркуна А.Д. Основи синтезу структури складних систем/О.Д. Цвіркун. - М.: Наука, 2018. - 197 с.
3. Сааті Т. Прийняття рішень. Метод аналізу ієрархій. / Сааті Т. - М.: Радіо і зв'язок, 2019.

Войцеховський Ю.Ю.
студент
Навчально-науковий інститут Інформаційних Технологій
Державній університет телекомунікацій, м. Київ
Науковий керівник: Золотухіна О. А.,
кандидат технічних наук, доцент, доцент кафедри Інженерії програмного забезпечення
Державного університету телекомунікацій, м.Київ

ОГЛЯД ПРОГРАМНИХ ЗАСОБІВ ДЛЯ ВЕДЕННЯ НАВЧАЛЬНОЇ КАРТКИ СТУДЕНТА

Важливою складовою навчального процесу є контроль студентської успішності, і для групування інформації про виконання учнями навчальної програми в освітніх установах створюються індивідуальні навчальні картки. З поширенням автоматизації паперовий формат документообігу замінюється електронним, і на поточний час для ведення студентських навчальних карток повсюдно використовуються текстові редактори.

Текстовий процесор «LibreOffice Writer» [1] є частиною програмного пакету для ведення цифрової документації «LibreOffice» та являє собою простий у освоєнні та використанні редактор. Головною перевагою «LibreOffice Writer» позиціонується доступність – продукт є безкоштовним та не потребує

для свого використання попередньої реєстрації. Однак в той же час текстовий редактор постачається разом із іншими компонентами пакету, функціонал яких може бути затребуваним потенційним користувачем лише частково або незатребуваним зовсім, та володіє обмеженими можливостями файлової конвертації.

Онлайн-редактор «Google Docs» [2] пропонується компанією «Google» та дозволяє здійснювати створення та редагування документів, не виходячи з браузеру. Ключовими особливостями «Google Docs» є автоматичне збереження змін, що виконуються користувачем, та хмарне збереження даних. Але потребу у постійному під'єднанні до мережі можна назвати головним недоліком текстового процесору, продуктивність якого буде прямим чином залежати від якості Інтернет-з'єднання користувача. Також розбіжною рисою можна вважати необхідність прив'язки до акаунту «Google», доступ до якого може бути втрачено за різних причин.

Кожен з наведених редакторів надає гнучкі можливості для створення стандартних документальних зразків, однак не позбавлений певних недоліків. Пропонується проектування десктопного додатку, що буде вузькоспеціалізованим для роботи з готовим шаблоном навчальної картки студента та не потребуватиме додаткової автентифікації за побічними обліковими записами.

Список використаних джерел:

1. Сайт «LibreOffice»: Текстовий процесор «LibreOffice Writer» [Електронний ресурс] - Режим доступу: https://www.libreoffice.org/discover/writer/ 19.05.2022
2. Сайт «Google»: Текстовий онлайн-процесор «Google Docs» [Електронний ресурс] - Режим доступу: https://www.google.com/intl/uk_ua/docs/about/ 19.05.2022

Позняк Я.І.
Студент 4 курсу
Державного університету телекомунікацій м. Київ
Науковий керівник: Боднарчук Андрій Петрович
д.т.н., професор кафедри Інженерії програмного забезпечення
Державного університету телекомунікацій, м.Київ

ОГЛЯД ЗАСОБІВ КОНТРОЛЮ СТАНУ ТА МІСЦЕПЕРЕБУВАННЯ ДОМАШНІХ ТВАРИН ТА СПОСОБИ ЇХ УДОСКОНАЛЕННЯ

За результатами соцопитування[1] на 2018 рік, близько у половини населення країни, а саме 57%, в будинку є домашня тварина. Переважну більшість становлять коти та собаки. Вибір домашньої тварини, в переважній більшості, залежить від господаря[2]. Так котів обирають більш інтровертні та спокійні люди. Більш розважливі люди обирають собак. Має значення і географічне положення. Так у сільській місцевості переважну більшість становлять тримачі собак, у той час коли кількість кошатників в два рази перевищує кількість собачників Переважна більшість, а саме 79%, сприймають домашню тварину, як члена сім'ї. Але в будь-якому випадку кожен хазяїн

переживає за стан та місцеперебування свого улюбленця. Інколи і стаються випадки коли господар не може цілодобово піклуватися про тварини. Адже в кожного з нас є список справ на день паралельно до доглядом за домашньою твариною. Наприклад робота. І не завжди можна дозволити працювати достатньо близько до дому, що може затруднювати догляд за своєю твариною. Тож корисно було б мати спосіб для відстеження місцезнаходження та стану свого улюбленця на відстані. Така інформація могла б допомогти господарям бути спокійнішими залишаючи оселю.

Напевно найефективнішими способами контролю місцеперебування тварини є повідець та вольєр. Але такі варіанти, мабуть, не підходять мешканцям міст, а також, певно, не підходить для котів. Іншим ефективним, але затратним способом є нашийники з GPS-навігатором. Це досить дієвий варіант, який значно спрощує догляд за твариною.

З того що зараз є на ринку можна виділити декілька нашийників. Як от Scollar Mini[3] - розумний модульний нашийник. Відстеження місцезнаходження тварин відбувається зі створенням карти їх прогулянок та місць, де вони найбільш часто люблять бувати. Додаток створює передбачувані маршрути можливого перебування улюбленців, ґрунтуючись на цих даних, щоб ви могли знати, де їх шукати в першу чергу. І це все без щомісячної абонплати за використання системи, що безумовно не може не радувати. Що правда нашийник не відстежує показники тварини, такі як пульс та температура тіла. Також з мінусів доволі висока ціна – в районі 200$.

Іншим достойним варіантом є EV-202 від тайванської компанії GPSM. Це розумний нашийник розроблений для відстеження місцяположення та захисту домашніх тварин. GPS, Bluetooth і технологія стільникового зв'язку об'єднані в одному пристрої для отримання точної інформації про місцеположення. Цей пристрій дарує спокій власникам домашніх тварин. За допомогою нього ви можете встановити межі безпечної зони, в якій може переміщуватіся тварина. Відслідковується переміщення за допомогою мобільного додатку та WEB-інтерфейсу. Зону переміщення можна обирати в додатку та спостерігати в режимі реального часу. Виробник також заявляє про вологостійкість нашийника. З мінусів можна виділити все ту ж неможливість спостерігати за фізичним станом домашнього улюбленця та доволі високу ціну.

Кожен з наведених нашийників надає велику кількість переваг для відстеження переміщень вашого улюбленця, однак не надає інформації про його стан. Пропонується проектування нашийника з доповненими функціями наведеними вище та якнайменше збільшувати собівартість готового продукту.

Список використаних джерел:

1. Сайт РБК-Україна [Електронний ресурс] – Режим доступу: https://styler.rbc.ua/ukr/
2. Сайт ZN,UA [Електронний ресурс] – Режим доступу: https://zn.ua/ukr/UKRAINE/
3. Сайт GT Racer [Електронний ресурс] – Режим доступу: https://gtracer.com.ua/scollar-mini

Гаврилець Максим Олександрович,
студент 5 курсу, групи КСДМ-51
(098)-880-22-54
megagavrilets@gmail.com
Науковий керівник: Ткаченко Ольга Миколаївна,
доктор технічних наук,
завідуюча кафедрою Комп’ютерної інженерії
Державного університету телекомунікацій, м. Київ

ЗАСТОСУВАННЯ ЗГОРТКОВИХ НЕЙРОМЕРЕЖ В РОЗПІЗНАВАННІ ЕЛЕМЕНТІВ

1. **Постановка задачі.**
   Розглянуто приклад побудови оптимальної структури згорткової мережі.
2. **Мета дослідження.**
   Розглянуто застосування згорткової нейронної мережі.
3. **Результати дослідження.**

Згорткова ж нейронна мережа за рахунок застосування спеціальної операції – власне згортки – дозволяє водночас зменшити кількість інформації, що зберігається в пам'яті інформації, за рахунок чого краще справляється з картинками більш високої роздільної здатності, і виділити опорні ознаки зображення, такі як ребра, контури або грані. На наступному рівні обробки з цих ребер і граней можна розпізнати повторювані фрагменти текстур, які далі можуть скластися в фрагменти зображення. По суті кожен шар нейронної мережі використовує власне перетворення. В результаті такого опрацювання ми можемо правильно класифікувати картинку або виділити на кінцевому етапі потрібний об'єкт на зображенні. Згорткові нейронні мережі застосовуються досить широко і в різних областях. Нижче ми розглянемо прості прикладні приклади того, як можна використовувати згорткову нейронну мережу в бізнесі.

Класифікація зображень і сигналів за допомогою нейронних мереж

Першим найбільш тривіальним завданням, яке навчилися вирішувати за допомогою нейронних мереж, стала класифікація зображень.

Класифікації за допомогою згорткової нейронної мережі активно застосовуються в медицині: можна навчити нейронну мережу класифікації хвороб або симптомів, наприклад, для МРТ-діагностики.

В агробізнесі розробляється і впроваджується методика аналізу та розпізнавання зображень, при якій дані отримують від відкритих супутників, таких як LSAT, і використовують для прогнозування майбутньої врожайності конкретних земель.

1) Розпізнавання об'єктів – object detection

Розпізнавання об'єктів на фото і відео за допомогою нейронних мереж застосовується в безпілотному транспорті, відеоспостереженні, системах контролю доступу, системах "розумного будинку" і так далі.

Зустрічається також масковане розпізнавання об'єктів з виділенням контуру, при якому ми також можемо отримувати чіткі контури об'єкта за допомогою згорткових нейронних мереж.

2) Нейронні мережі для розпізнавання облич і людей

Розпізнавання облич означає можливість виділяти обличчя на зображеннях. А потім, за допомогою нейромереж, розпізнавати обличчя конкретної людини. Також нейронні мережі можна використовувати для виділення людей або окремих частин тіла людини на фото або відео, для побудови їхніх скелетів, поз. Такий підхід застосовується, наприклад, для відеоаналітики.

3) Тривимірна реконструкція облич і об'єктів по фотографії за допомогою згорткових нейронних мереж

На даний момент існує кілька конкуруючих моделей, що дозволяють отримати тривимірні моделі особи (3DMM) всього по одній фотографії. Крім реконструкції облич згорткові мережі застосовують також для реконструкції інших тривимірних об'єктів по фото.

4) Розпізнавання мови й аналіз емоційної тональності тексту

Згорткові нейронні мережі можна застосовувати не тільки для вирішення завдань комп'ютерного зору. Наприклад, недавно Facebook AI Research виклала у відкритий доступ wav2letter ++ – свою технологію розпізнавання мови, засновану на згортковій нейроній мережі.

4. Висновки та перспективи.

Згорткова нейронна мережа на сьогодні – "робоча конячка" в області нейронних мереж. Використовується переважно для вирішення завдань комп'ютерного зору, хоча може застосовуватися також для роботи з аудіо і будь-якими даними, які можна представити у вигляді матриць.

Перспективні напрями подальших досліджень стосовно даної проблеми можуть бути пов’язані з розробкою інтелектуальної системи прогнозування результатів фізичного стану у сфері фізичної культури і спорту.

Список використаних джерел

1. https://evergreens.com.ua/ua/articles/cnn.html

Гаврилець Максим Олександрович,
студент 5 курсу, групи КСДМ-51
(098)-880-22-54
megagavrilets@gmail.com
Науковий керівник: Ткаченко Ольга Миколаївна,
доктор технічних наук,
завідуюча кафедрою Комп’ютерної інженерії
Державного університету телекомунікацій, м. Київ

ПРОБЛЕМАТИКА ВИКОРИСТАННЯ ДРОНІВ У ЛОГІСТИЦІ

1. Постановка задачі.

Аналізуються переваги та недоліки застосування дронів у логістиці.

2. Мета дослідження.

Оцінюється перспектива зміни логістичних систем відповідно до впровадження дронів.

3. Результати дослідження.

Використання дронів у логістичному ланцюжку стало одним з основних

завдань компаній-гігантів таких, як Google, Amazon. Кожна з них уже спроектувала свій власний літальний перевізник та вже проводить випробування. У чому ж основна причина використання дронів у ланцюзі постачання? Чи вигідно це з економічної точки зору, чи це просто новий спосіб залучити до себе клієнтів? Відповісти на це питання можна лише проаналізувавши всі «за» і «проти» використання дронів у логістиці.

Переваги

1. Економія коштів.

Співзасновник компанії Kiva Systems, що займається розробкою БПЛА, оцінив вартість доставки вантажами дронами не більше 2 кг «на останній милі»: вона становить $0,1. У порівнянні – наземна доставка вантажу, аналогічного за параметрами, складається від $2 до $8.

При цьому враховувалися такі змінні: витрати на розгортання БПЛА – угруповання, технічну та інформаційну підтримку, а також % від замовлень, які можуть бути оброблені, використовуючи БПЛА. З економії випливає великий прибуток.

2. Виняток «людського фактора»

Подібні апарати не потребуватимуть дорогих систем життєзабезпечення. До того ж дрони можуть бути безпечнішими, якщо врахувати, що більшість аварій літаків відбувається через «людський фактор». Автоматизація виробничих та логістичних ланцюгів – головна мета використання безпілотників.

3. Екологічність

Транспортні засоби дуже сильно забруднюють довкілля. Уряд США вже давно лобіює «зелене виробництво», стимулюючи розвиток цього напряму шляхом запровадження високих податків на промислові відходи. Використання дронів – це абсолютно екологічний процес.

4. Гнучкість у ланцюгу поставок

Автономність безпілотних апаратів дозволяється коригувати курси у разі потреби, форс-мажорних обставин або за певних вимог клієнта. Швидкість реагування зміну умов замовлення дуже висока.

Недоліки

1. Конфіденційність та безпека

Використання дронів для доставки товару по місту – це найбільш відчутне та вражаюче майбутнє в галузі логістики. Але також доведеться зіткнутися з безліччю проблем. Через те, що проблеми конфіденційності та безпеки множаться у густонаселеному міському середовищі, найскладнішим, з погляду норм моралі та моральності, є створення необхідних умов для логістичної інфраструктури.

2. Законопроекти

Існує низка законопроектів, які обмежують польоти безпілотників у повітряному просторі. Також необхідна реєстрація цих апаратів на державному рівні, причому, ця процедура необхідна для дронів, що належать людям, які використовують їх для розваги.

3. «Проблеми у повітрі»

Дрони не врізалися у стіну і навіть не зіткнулися із законодавчою базою,

а з птахами. Птахи можуть потрапити в лопаті дрони, при цьому загине і птах, а також пошкодитися БПЛА разом із вантажем. З цього відразу три проблеми виникає, які потрібно буде вирішити: заподіяну шкоду живій природі, ремонт апарат, незадоволеність клієнта.

4. «Проблеми землі»

Вандалізм - головна проблема держав. Викрадення дроном, стрілянина по них – це ризики, які виникнуть. І головне, що відстежити дрон під час викрадення, можна буде лише за останнім місцем розташування, тому що завжди є сліпі зони за умови використання камери.

5. Зіткнення з природою

Машина, поїзд можуть долати погодні умови тією чи іншою мірою. На жаль, вага безпілотників дуже маленька, щоб протистояти вітру чи дощу. Зміна погодних умов спричиняє зміну в часі та швидкості польоту.

4. Висновки та перспективи.

Як видно, проблем багато: законодавча база, великий обсяг вкладень. Але переваги колосальні: економія на масштабі у довгостроковій перспективі, а також автоматизація логістичних процесів. Найближчим часом дрони не з'являться над головою. Проте напрямів розвитку дуже багато. І протягом 5 років безпілотні літальні апарати все-таки доставлятимуть найнеобхідніше людям.

Список використаних джерел

1. https://cyberleninka.ru/article/n/problematika-ispolzovaniya-bespilotnyh-letatelnyh-apparatov-dronov-v-logistike

Тарнагродський Ейнар Ярославович
Студент 5 курсу,групи КСДМ-51
(099)-272-36-76
tarnagrodskiy438@gmail.com
Навчально-науковий інститут інформаційних технологій
Державний університет телекомунікацій, м. Київ

АЛГОРИТМ ЗАПОБІГАННЯ НЕСПРАВНОСТЕЙ В ІНТЕЛЕКТУАЛЬНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

Інтелектуальні комп'ютерні системи (ІКС) – це клас автоматизованих систем оброблення інформації на основі ЕОМ, які моделюють розумові процеси, притаманні людині при прийняті рішень у різних галузях соціально-економічної сфери суспільства.[1, с. 10]. Інтелектуальні комп'ютерні системи вже значно впливають на те, як люди працюють і живуть. У міру зростання споживання продуктів і послуг, створених на основі і машинного навчання, необхідно вживати спеціальні заходи, щоб захистити не тільки клієнтів і їх дані, але і самі ІКС від порушення працездатності. Запобігання несправностям стосуються захисту продуктів і служб, створених на основі інтелектуальних комп'ютерних систем, від складних і витончених шкідливих атак, які організовують як окремі особи, так і групи зловмисників.

Постановка задачі. Інтелектуальні комп'ютерні системи з кожним роком набувають все більшого розвитку та спроможності вирішувати більший обсяг

завдань, але вони мають свої унікальні проблеми які шкодять їх працездатності, а також потребують інструкцій, розробки та вдосконалення систем захисту, стандартизації міжнародними організаціями по стандартизації з електричних та електронних виробів й технологій. Усунення проблем зі стандартними векторами програмних атак як і раніше має велике значення. Але цього недостатньо для ефективної боротьби з загрозами для штучного інтелекту і машинного навчання. Важливо створити інфраструктуру і використовувати нові підходи, які зможуть усунути недоліки в розробці і експлуатації служб на основі інтелектуальних систем і машинного навчання.

Метою дослідження. Метою дослідження є виявленні розповсюджених проблемах при роботі, навчанні та сприйнятті інформації ІКС та визначення методів запобігання несправностей.

Результати дослідження. ІКС повинні вміти виявляти аномальні вхідні дані і запобігати маніпуляціями або спробам спотворення результатів. Їх слід проектувати таким чином, щоб вони могли протистояти сумнівним вхідними даними, що потенційно суперечать місцевим законам, етичним нормам і цінностям, які транслюються конкретним співтовариством. ІКС потрібно надати можливість визначати, коли взаємодія з користувачем виходить за рамки прийнятного сценарію. Такі атаки потрібно розглядати на одному рівні з атаками типу "відмова в обслуговуванні", оскільки після них виникає потреба перенавчання і виправлення помилок, задля неможливості впливу подібним шляхом на ІКС[2].

Методи запобігання впливу аномальних вхідних даних на роботу ІКС:

- виявлення окремих користувачів, поведінка яких відхиляється від норми, яка встановлена на основі аналізу безлічі подібних великих груп людей. Наприклад, вони занадто швидко набирають текст або реагують на дії алгоритму, проявляють цілодобову активність або запускають ті елементи системи, з якими інші користувачі не взаємодіють;
- визначення моделі поведінки користувачів, які є індикаторами навмисних пробних атак і початку поетапного шкідливого проникнення в ІКС;
- фіксація всіх випадків, узгодженого виконання однакових дій кількома користувачами. Наприклад, навмисна відправка одного і того ж незрозумілого запиту, або раптові сплески активності кількості користувачів у певних частинах ІКС;
- встановлення автентифікації між агентами і їх привілеїв доступу до даних.

Інтелектуальна комп’ютерна система повинна діяти неупереджено і враховувати всю інформацію без дискримінації окремої групи користувачів або достовірних вихідних даних. Але для цього в системі спочатку повинна бути закладена концепція упередженого ставлення. Якщо не навчити систему розпізнавати упередженість, вона буде нестійкою до неправильних тверджень.

Для вирішення проблем упередженого ставлення:

- система повинна вміти виявляти користувачів з якими в минулому був негативний досвід взаємодії, і проявляти відповідну обережність;
- система повинна вміти розпізнавати відхилення від норми в наборах даних, на яких вона навчається. Замість роботи з довжинами і зсувами

перевірки буфера та кордонів орієнтуються на спеціально помічені слова, зібрані з великої кількості джерел. Історія спілкування і контекст, в якому використовуються слова, також мають ключове значення. Методи ешелонованого захисту створюють кілька рівнів безпеки.

У багатьох опублікованих технічних документах розглядається теоретична можливість несанкціонованої зміни моделі [2] або класифікатора, а також вилучення або крадіжки інформації зі служб, в яких зловмисники мають доступ як до набору навчальних даних, так і до змістовного розуміння використаної моделі. Основна проблема тут полягає в тому, що зловмисники, які контролюють набори тренувальних даних, можуть маніпулювати всіма класифікаторами. І з часом для класифікаторів ці вхідні дані стають "надійними" через нездатність відрізнити шкідливі аномальні дані від справжніх.

Запобігати можливості зміни моделі допоможе впровадження концепції, яка пов'язана зі здатністю виявляти і відхиляти навмисно введені шкідливі навчальні дані або вхідні дані від користувачів до того, як вони зроблять негативний вплив на поведінку класифікатора.

В особливо важливих сценаріях інтелектуальна система повинна мати можливість проводити аналітичну експертизу і вести журнал безпеки. Це дозволить забезпечити цілісність, прозорість і контрольованість, а також надати докази у випадках коли це необхідно. Ключовим службам системи будуть потрібні результати аудиту і трасування подій на рівні алгоритму, за допомогою яких розробники зможуть перевірити записаний стан певних класифікаторів, який призвів до помилкового рішення. Засоби трасування подій мають відстежувати взаємопов'язані базові дані для прийняття рішень:

- період часу, в який відбулася остання навчальна подія;
- позначка часу для останнього запису набору даних, на базі якого відбувається навчання;
- Вагомість і рівні достовірності основних класифікаторів, що використовуються для прийняття рішень;
- перелік класифікаторів або компонентів, що беруть участь в ухваленні рішення;
- остаточне важливе рішення, до якого прийшов алгоритм.

Ще один аспект аналітичної експертизи, необхідної для інформаційної системи і машинного навчання є виявлення злому. ІКС повинна розпізнавати упереджену поведінку і не допускати її негативний вплив, але також системі необхідна можливість аналітичної експертизи, щоб допомогти інженерам виявляти такі атаки і реагувати на них. Поєднання можливості аналітичної експертизи з методами візуалізації даних дозволять проводити аудит налагодження алгоритмів запобігання несправностей в ІКС.

Висновки та перспективи. Отже, можна дійти до висновку, що ІКС дуже швидко розвиваються та набувають дедалі більшого розповсюдження, а також отримують спроможність для вирішення більш складних задач. Але вони мають свої недоліки та уразливості, що вимагає створення сценаріїв роботи, вирішення проблем правильного усвідомлення вхідних даних, захисту від зміни моделі та класифікаторів, захисту збереженої та конфіденційної інформації,

необхідності проведення аналітичних експертиз та можливості виявлення злому систем ІКС.

Список використаних джерел:

1. Довбиш А.С. Основи проектування інтелектуальних систем: Навчальний посібник / Довбиш А.С. Суми: СумДУ, 2009. – 171 с.
2. Атака на машинне навчання за допомогою загальних прикладів [Електронни ресурс] – Режим доступу: *https://openai.com/blog/adversarial-example-research/*

Миколаєнко Дмитро Олександрович
Студент 5 курсу,групи КСДМ-51
Державний університет телекомунікацій, м. Київ
Навчально-науковий інститут інформаційних технологій
(096)-146-81-10
mikolaenko17.dima@gmail.com

РОЗГЛЯД VPN ТА АНОНІМАЙЗЕРІВ В ЯКОСТІ ЗАСОБІВ БЕЗПЕЧНОГО ВИКОРИСТАННЯ НЕЗАХИЩЕНИХ МЕРЕЖ

Віртуальна приватна мережа Virtual Private Network (VPN) - це технології, які дають змогу забезпечувати одне або ж відразу кілька мережевих з'єднань поверх іншої мережі, наприклад, Інтернету.

Дане з'єднання має вигляд зашифрованого тунелю, який пов'язує безпосередньо комп'ютер користувача і віддалений сервер, що дозволяє не тільки, але також зашифрувати свій трафік. Інакше кажучи, таким чином ви зумієте завантажувати що завгодно і звідки завгодно, і про це ніхто не дізнається.

Постановка задачі. Сучасний розвиток інформаційних технологій і, зокрема, мережі Internet, призводить до необхідності захисту інформації, переданої в рамках розподіленої корпоративної мережі, що використовує мережі відкритого доступу. Однак Інтернет є незахищеною мережею, тому доводиться винаходити засоби захисту конфіденційних даних, переданих по незахищеній мережі.

Мета дослідження. Метою дослідження є розгляд VPN та анонімайзерів в якості засобу безпечного використання незахищених мереж.

Результати дослідження. Скорочено від “Virtual Private Network” (віртуальна приватна мережа), **VPN створює безпечне з’єднання між вами та інтернетом**. Це забезпечує додатковий рівень конфіденційності та анонімності, щоб ви мали змогу:

- Приховати свою інтернет-активність та місцезнаходження, щоб вас неможливо було відстежити (особливо в публічних WiFi-мережах)
- Обійти онлайн-цензуру та вільно користуватися інтернетом
- Безпечно та анонімно завантажувати торренти без втрати швидкості
- Розблоковувати стрімінгові платформи, такі як Netflix, Disney+ та інші

Що таке VPN-підключення і навіщо воно потрібне

Дана технологія має на увазі під собою захищену мережу, створену поверх

незахищеною мережі. VPN-клієнт, використовуючи публічну мережу, через спеціальні протоколи підключається до VPN-сервера. Сервер приймає запит, перевіряє справжність клієнта і після цього передає дані. Це забезпечується засобами криптографії.

Можна налаштувати такі види VPN-підключень, як перераховані нижче.

Віртуальна приватна мережа PPTP

PPTP - Point-toPoint Tunneling Protocol -туннельний протокол типу «точка-точка», який допоможе встановити захищений тунель в незахищеній мережі. Він є найбільш популярним способом VPN-підключення, проте багато інтернет-провайдери блокують роботу таких додатків.

Віртуальна приватна мережа OpenVPN

OpenVPN - являє собою вільну реалізацію даної технології з наданням відкритого коду для створення своїх зашифрованих каналів за типами «точка-точка» або «сервер-клієнт». Останній дозволяє використовувати в якості VPN-сервера інший комп'ютер. Однак для настройки тунелю потрібна установка спеціального програмного забезпечення укупі зі знаннями для роботи з ним.

Віртуальна приватна мережа L2TP

L2TP (Layer 2 Tunneling Protocol) - найбільш трудомісткий для настройки вид VPN-тунелю, але дозволяє створювати його з заданими пріоритетами доступу, роблячи найбільш захищеним.

І хоча VPN не є в прямому сенсі анонімайзерами, проте вже сьогодні більшість сайтів, що надають послуги CGI-ргоху, пропонують придбати свій власний VPN-канал. Ця технологія набирає обертів, так що цілком ймовірно, що незабаром кількість звичних анонімайзерів буде зводитися до необхідного мінімуму.

Існує декілька засобів, один з яких це анонімайзери або проксі-сервера, вони приховують дані про комп'ютер або користувача в локальній мережі від віддаленого сервера. Розглянувши принцип роботи проксі-серверів, можемо сказати, що анонимайзер завжди розриває прямий ланцюг зв'язку і стає посередником між веб-браузером і потрібним веб-сервером. У сфері кібербезпеки анонімізуючий проксі-сервер − це інструмент, який можна використовувати для того, щоб зробити онлайн-діяльність невідстежуваною або анонімною. Ці проксі, по суті, діють як посередницькі "шлюзи" між користувачем Інтернету та їхнім місцем призначення, як і VPN. Проте VPN − це технологія, яка об'єднує довірені мережі, вузли і користувачів через відкриті мережі, яким немає довіри. Технологія, яка набуває все більшого поширення серед не тільки технічних фахівців, а й серед звичайних користувачів, яким також потрібно захищати свою інформацію (наприклад, користувачі Internet-банків або Internet-порталів). На відміну від анонімайзерів, VPN шифрують онлайн-трафік. Анонімайзер, в свою чергу, тільки маскує вашу IP-адресу, він не може захистити вас від відстеження вашим постачальником послуг Інтернету або іншими третіми сторонами. Проксі-севери працюють на рівні додатків, тоді як VPN працюють на рівні операційної системи. Іншими словами, VPN може охоплювати весь Інтернеттрафік, що надходить з комп’ютера користувача, тоді як проксі-сервер покриває лише трафік, що надходить із певного браузера чи програми. Користувачі VPN можуть використовувати техніку, яка називається

розділеним тунелюванням, щоб вибрати, який трафік буде маршрутизуватися через їх VPN. Так будь-який інструмент, який перенаправляє веб-трафік клієнта для захисту його конфіденційності, швидше за все, вплине на швидкість Інтернету. Однак, оскільки VPN також шифрують дані клієнта, вони можуть бути повільнішими за анонімайзери. Компроміс полягає в тому, що VPN часто пропонують більш надійну безпеку та конфіденційність, ніж анонімайзери.

Баришев Юрій Ігорович,
студент 5 курсу, групи КСДМ-51
Державного університету телекомунікацій
(067) 972 13 58
yuriibaryshev@gmail.com
Науковий керівник: Кирпач Людмила Андріївна
к.т.н., доцент, завідувач кафедри космічних систем та комплексів і супутникових телекомунікацій
Державного університету телекомунікацій, м. Київ

ВИКОРИСТАННЯ СУПУТНИКОВОГО ІНТЕРНЕТУ В УМОВАХ ВІЙНИ

Ця теза розповідає про функціонування супутникового інтернету та як його можна використовувати на територіях з зруйнованою телекомунікаційною інфраструктурою

Постановка задачі.

Під час військових дій виникають труднощі з багатьма речами, зокрема з телекомунікацією, але використання супутникового інтернету може вирішити цю проблему.

Мета дослідження.

Дослідити використання супутникового інтернету на територіях з зруйнованою телекомунікаційною інфраструктурою

Результати дослідження.

У зв’язку з військовими діями на території України, руйнуванням будівель та телекомунікаційної інфраструктури багато людей, важливих підприємств та державних служб залишаються без доступу до інтернету та засобів зв’язку. Вони не мають змоги зв’язатися з рідними та отримати доступ до інформації, адже мобільний зв’язок може не працювати як і кабельний інтернет. Для вирішення цієї проблеми можна використовувати засоби доступу до супутникового інтернету.

Однієї з провідних компаній надання послуг супутникового інтернету є компанія SpaceX, що розроблює глобальну супутникову мережу Starlink. Вже зараз люди мають змогу отримати доступ до швидкого інтернету з низькими затримками, в тому числі і на території нашої країни. В Україну вже доставлені тисячі терміналів та цими послугами щодня користуються близько 150000 користувачів.

Система Starlink передає сигнал з супутника на наземну станцію, а від неї на користувацький термінал. Так як на Україні немає своєї станції, українці використовують термінали завдяки станціям у Польщі та Німеччині. Через це якість зв’язку на сході гірша ніж на заході. Згідно тестам максимальна

швидкість яка була зафіксована є 278 Мбіт та затримка сигналу до 75 мс. SpaceX каже, що коли повністю закінчіть свій проект максимальні затримка буде на рівні 20 мс.

Однак використання Starlink все ж дорожче аніж кабельного інтернету, однак там де зруйнована кабельна інфраструктура він дозволяє швидко відновити інтернет-доступ.

Висновки та перспективи

Супутниковий інтернет вдало використовується та вирішує критичні проблеми з зв'язком та інтернетом. Він є дорогим та менш швидким ніж інтернет за допомогою кабелю, але може використовуватися там, куди немає змоги його дотягти, як наприклад у сільських місцевостях

Список використаних джерел:

1. https://www.starlink.com/
2. https://www.epravda.com.ua/rus/news/2022/05/2/686538/
3. https://www.bbc.com/ukrainian/news-61168415

Клочков Михайло Васильович
студент 5 курсу, групи КСДМ-51
(095)592-1560
mihey-av@ukr.net
Науковий керівник: Ткаченко Ольга Миколаївна,
Доктор технічних наук, доцент
Завідувачка кафедри Комп'ютерної інженерії
Державного університету телекомунікацій м. Київ

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ ДИСПЕТЧЕРИЗАЦІЇ В ЦЕНТРАХ ЕКСТРЕНОЇ МЕДИЧНОЇ ДОПОМОГИ

Сьогодні інформатизація медицини є одним із пріоритетних напрямків розвитку охорони здоров'я. Особлива увага останнім часом приділяється збереженню інформації про пацієнтів, статистичному аналізу і швидкому доступу до даних тощо. Важливе значення також надається підвищенню ефективності праці лікаря, уникненню помилок при діагностиці й записі інформації до баз даних, стандартизації основних процедур. Суттєво підвищити ефективність діяльності всієї медичної установи можливо шляхом впровадження автоматизованих інформаційних технологій і систем [1].

Постанова задачі. Ознайомити слухачів з темою автоматизацію процесів диспетчеризації в центрах екстреної медичної допомоги.

Мета дослідження. Донести інформацію про автоматизацію процесів диспетчеризації в центрах екстреної медичної допомоги.

1. Історія автоматизації процесів диспетчеризації.
2. Що таке автоматизація процесів диспетчеризації.
3. Структура автоматизації процесів диспетчеризації.

Результат дослідження.

Автоматизація процесів обробки викликів, що надходять за телефонним номером 103 має багату історію та різні підходи автоматизації. З приходом ери інформатизації та комп'ютеризації багато процесів диспетчеризації автоматизуються за допомогою програмно-апаратних комплексів.

Перші кроки до впровадження автоматизації процесів прийняття виклику від населення міста Києва та передачі їх виїзним бригадам були ще з 1963 року, засобами телефонного та радіозв'язку.

Наступним суттєвим кроком до автоматизації було впровадження в кінці 1999 року з використанням ПЕОМ, серверного та комутаційного обладнання автоматизованої інформаційно-диспетчерської системи «Швидка медична допомога». Це дозволяло значно зменшити час на прийняття викликів від населення диспетчером 03 та передачу їх на підстанцію в автоматичному режимі; бачити стадії їх виконання. Також з'явилась можливість швидко формувати звіти використовуючи ПЕОМ. Але як і раніше передача виклику на бригаду здійснювалась диспетчером підстанції за допомогою радіозв'язку.

Лише з впровадженням Автоматизованої Інформаційно-Диспетчерської Система «Швидка Медична Допомога», інформаційно-аналітичної системи «Єдиний медичний простір» (далі – АІДС «ШМД») за допомогою сучасних інформаційно-телекомунікаційних технологій було повністю автоматизовано всі технологічні процеси пов'язані з прийомом викликів по 103, обробкою за територіальними ознаками та передачі їх безпосередньо виїзним бригадам на мобільний термінал бригади (далі – МТБ) в автоматичному режимі, контролюючи при цьому всі стадії їх виконання. Ці нововведення значно скоротили час від моменту надходження дзвінка на 103 до моменту виїзду бригад екстреної (швидкої) медичної допомоги з подальшою візуалізацією переміщення бригади до місця виклику на карті міста Києва. Відображення бригад на карті дозволяє направити на виклик найближчу вільну бригаду, що суттєво зменшує час доїзду, особливо в години пік.

АІДС «ШМД» являє собою складний програмно-технічний комплекс, створений на базі найсучасніших інформаційних та телекомунікаційних технологій. Автоматизуються процеси служб диспетчеризації викликів та робочі місця адміністративного апарату Центру екстреної медичної допомоги та медицини катастроф міста Києва (далі – Центр ЕМД та МК) до складу яких входять : диспетчерська по прийому викликів "103", диспетчерська по передачі викликів у відділення, диспетчерські 16-ти відділень та відділу медицини катастроф, "Відділ вільних ліжок та госпіталізацій", "Відділ статистики ", "Довідково-інформаційна служба "1503", "Консультативно-інформаційна служба "1583", Центр оперативної підтримки громадян з вадами слуху та мови, Консультативно-телеметричний центр, робочі місця апарату управління та рухомий склад Центру ЕМД та МК і відділення екстреної (швидкої) медичної допомоги з надання медичної допомоги та перевезення психічно хворих .

АІДС «ШМД» забезпечує управління технологічним процесом оперативної роботи Центру ЕМД та МК в режимі реального часу. Автоматизуються процеси прийому викликів "103", аналіз викликів за приводом та територіальними ознаками, передача викликів у відділення, процес ведення виклику та управління виїзними бригадами, процес передачі виклику на МТБ, відображення стану оперативної роботи всіх відділень та всього центру загалом, статистичної обробки інформації.

Структура АІДС «ШМД» складається з наступних модулів:

- цифрової телекомунікаційної системи;

- головного та резервного серверу баз даних;
- серверу обробки статистичних даних та баз даних координат рухомих об’єктів (РО);
- серверу реєстрації мовної інформації;
- серверу інтеграції цифрової телекомунікаційної системи з інформаційною системою;
- зовнішнього сховища;
- робочих станцій користувачів системи;
- пристроїв передачі даних місця розташування РО;
- мобільних терміналів бригад;
- активного та пасивного мережевого та телекомунікаційного обладнання.

Захищені канали зв’язку АІДС «ШМД» побудовані за допомогою корпоративної комп’ютерної мережі з використанням протоколів IPsec [1], яка об’єднує оперативно-диспетчерський відділ зі всіма відділеннями екстреної (швидкої) медичної допомоги, розташованими в різних районах міста Києва. Бездротове з’єднання рухомих об’єктів забезпечує оператор мобільного зв’язку.

Структурна схема побудови АІДС наведена на Рисунку 1.

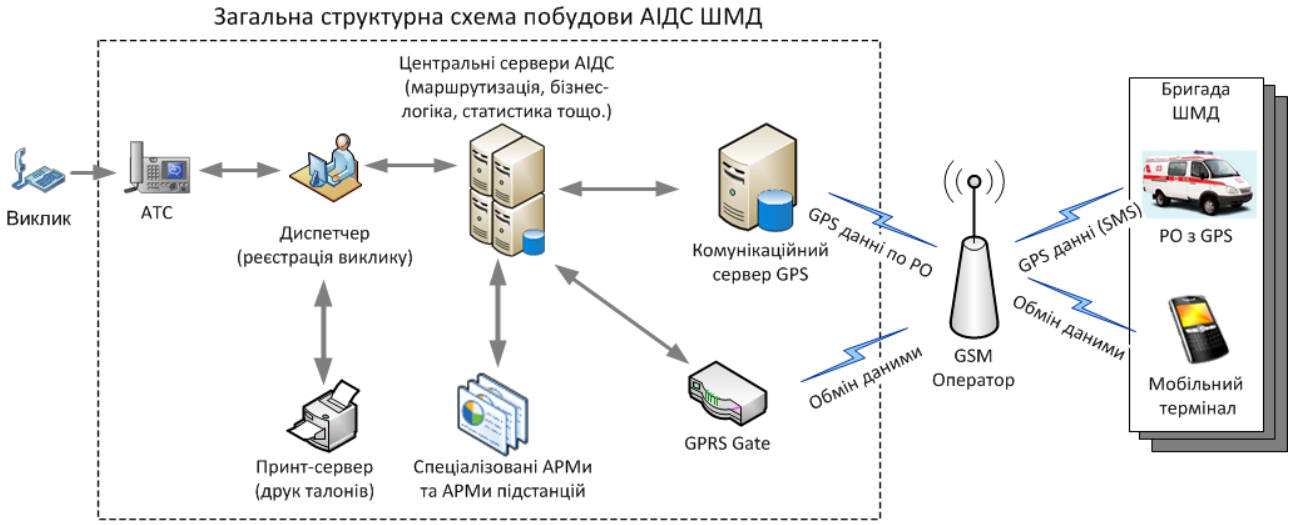

Рис. 1. Структурна схема побудови АІДС

Висновки та перспективи. Велику увагу приділено резервуванню систем та каналів зв’язку у випадку надзвичайних ситуацій. Із них можна виділити:

- резервування потужностей та інформації;
- резервування енергозабезпечення засобами безперебійного живлення та дизель-генератором;
- резервування каналів зв’язку безпосереднім зв’язком та радіозв’язком.

Всі ці заходи спрямовані на функціонування АІДС «ШМД» в режимі 24 години на добу 7 днів на тиждень 365 днів на рік для забезпечення безперервного доступу жителів міста Києва до послуг за телефоном 103.

Перспективами розвитку автоматизації процесів диспетчеризації

являються програмно-апаратні комплекси, які будуються з використанням сучасних інформаційно-телекомунікаційних технологій та у зв'язці з сучасним програмним забезпеченням забезпечать ще більшу автоматизацію з використанням алгоритмів та протоколів, що обробляються з використанням хмарних технологій. Все це в комплексі забезпечить гарантований прийом викликів, зменшення часу прийому виклику при надходженні даних про номер телефону і позиціювання абонента на місцевості в автоматичному режимі, обробку алгоритму опитування та автоматичного визначення екстреності виклику під час опитування.

Список використаних джерел:

1. Інформаційні технології у сфері охорони здоров'я : монографія / Л.Б. Ліщинська, С.А. Яремко, К.В. Копняк, І.О. Гулівата, Л.П. Гусак ; за заг. ред. Л.Б. Ліщинської. – Вінниця : видавничоредакційний відділ ВТЕІ КНТЕУ, 2018. – 240 с.
2. Інтернет-джерело https://uk.wikipedia.org/wiki/IPsec.

Тарнагродський Ейнар Ярославович
Студент 5 курсу,групи КСДМ-51
(099)-272-36-76
tarnagrodskiy438@gmail.com
Навчально-науковий інститут інформаційних технологій
Державний університет телекомунікацій, м. Київ

СИСТЕМИ ТА ЗАЛЕЖНОСТІ МОДЕЛЮВАННЯ ЗАГРОЗ ARTIFICAL INTELLIGENCE, MACHINE LEARNING

Традиційне пом'якшення загроз безпеці AI,ML важливіше, ніж будь-коли. Вимоги, встановлені життєвим циклом розробки безпеки є суттєвими для створення основи безпеки продукту. Неможливість подолати традиційні загрози безпеці допомагає увімкнути атаки, пов'язані з штучним інтелектом і машинним навчанням, які у програмному, так і в фізичному доменах, а також робить компроміс тривіальним у нижньому стеку програмного забезпечення.

Постановка задачі. Сховища навчальних даних та систем на яких вони розміщені, є частиною сфери моделювання загроз. Найбільшою загрозою безпеці в машинному навчанні сьогодні є отруєння даних через відсутність стандартних засобів виявлення та пом'якшення в цьому просторі, у поєднанні із залежністю від недовірених, або неконтрольованих загальнодоступних наборів даних як джерел навчальних даних. Відстеження походження та походження даних має важливе значення для забезпечення їх достовірності та уникнення циклу навчання "garbage in, garbage out". Якщо не пом'якшити, атаки на системи штучного інтелекту та машинного навчання то вони можуть потрапити у фізичний світ. Будь-який сценарій, який можна використати, щоб психологічно або фізично завдати шкоди користувачам, є катастрофічним ризиком для продукту, або послуги.

Метою дослідження. Метою дослідження є визначити розповсюджені проблеми безпеки при роботі з сховищами навчальних даних та системами, а

також формування пом’якшувальних дій для збереження, захисту даних та системи.

Результати дослідження. У атаках у стилі збурень зловмисник приховано модифікує запит, щоб отримати бажану відповідь від моделі, розгорнутої у виробництві [1]. Це порушення цілісності введення моделі, що призводить до атак у стилі fuzzing, коли кінцевий результат не обов’язково є порушенням доступу або Exchange Online Protection, але натомість ставить під загрозу ефективність класифікації моделі. Це також може проявлятися в тому, що зловмисники використовують певні цільові слова таким чином, щоб AI блокувало їх, фактично відмовляючи в наданні послуг легальним користувачам з іменем, що відповідає «забороненому» слову.

Цілеспрямована неправильна класифікація, у цьому випадку зловмисники генерують зразок, який не входить до вхідного класу цільового класифікатора, але модель його класифікує як конкретний вхідний клас. Змагальна вибірка може здаватися людським очам як випадковий шум, але зловмисники мають певні знання про цільову систему машинного навчання, щоб генерувати білий шум, який не є випадковим, але використовує деякі специфічні аспекти цільової моделі. Супротивник дає вхідний зразок, який не є легітимним, але цільова система класифікує його як легітимний клас. Також варіант випадкових помилок класифікацій, коли цільова класифікація зловмисника може бути будь-якою іншою, ніж класифікація законного джерела. Атака, як правило, включає випадкове введення шуму в вихідні дані, які класифікуються, щоб зменшити ймовірність використання правильної класифікації в майбутньому [2].

Пом’якшення:

- Підсилення стійкості протиборства з використанням впевненості моделі, викликаної змагальною підготовкою [3], у таких випадках слід використовувати Highly Confident Near Neighbor (HCNN), структуру, яка поєднує інформацію про довіру та пошук найближчого сусіда, щоб підсилити конкурентну стійкість базової моделі. Це може допомогти розрізняти правильні та неправильні прогнози моделі в околиці точки, відібраної з базового розподілу навчання.
- Причинний аналіз, керований атрибуцією, слід вивчати зв’язок між стійкістю до протиборчих збурень і поясненням на основі атрибуції індивідуальних рішень, створених моделями машинного навчання. Вони повідомляють, що змагальні дані не є надійними в просторі атрибуції, тобто маскування кількох функцій з високою атрибуцією призводить до зміни нерішучості моделі машинного навчання на прикладах із змагальністю. Навпаки, природні вхідні дані є надійними в просторі атрибуції.

Зниження впевненості, зловмисник може створювати вхідні дані, щоб знизити рівень достовірності правильної класифікації, особливо в сценаріях із високими наслідками. Це також може мати форму великої кількості помилкових спрацьовувань, призначених для перевантаження адміністраторів або систем моніторингу шахрайськими попередженнями, які неможливо відрізнити від законних [2].

Пом’якшення:

- Використовувати вищезазначені дії, а також для зменшення гучності сповіщень з одного джерела можна використовувати регулювання подій.

Цільове отруєння даних, мета зловмисника – забруднити модель машини, створену на етапі навчання, щоб прогнози щодо нових даних були змінені на етапі тестування [1]. Під час цілеспрямованих атак отруєння зловмисник хоче неправильно класифікувати конкретні приклади, щоб змусити вжити або пропустити конкретні дії. Або невибіркове отруєння даними, мета якого полягає в зіпсувані якості, або цілісності набору даних, які атакуються. Багато наборів даних є загальнодоступними, недовіреними та неналежними, тому це створює додаткові занепокоєння щодо можливості виявлення таких порушень у цілісності даних, навчання на несвідомо скомпрометованих даних. Після виявлення, сортування має визначити обсяг даних, які були порушені, та помістити на карантин, або перенавчати.

Пом’якшення:

- Визначте датчики аномалій, щоб дивитися на щоденний розподіл даних і сповіщати про зміни.
- Перевірка введених даних, як очищення, так і перевірка цілісності.

Атаки інверсії моделі. Приватні функції, які використовуються в моделях машинного навчання, можна відновити [1]. Це включає відновлення приватних навчальних даних, до яких зловмисник не має доступу. У біометричній спільноті також відомі як атаки підйому на гору. Це досягається шляхом знаходження вхідних даних, які максимізують рівень довіри, що повертається, за умови відповідності класифікації цілі [4].

Пом’якшення:

- Інтерфейси до моделей, навчені на основі конфіденційних даних, потребують сильного контролю доступу.
- Запити про обмеження швидкості дозволені моделлю.
- Реалізуйте шлюзи між користувачами, абонентами та фактичною моделлю, виконуючи перевірку введених даних для всіх запропонованих запитів, відхиляючи все, що не відповідає визначенню моделі щодо правильності введення, і повертаючи лише мінімальний обсяг інформації, необхідний для використання.

Атака висновку про членство, зловмисник може визначити, чи був даний запис даних частиною навчального набору даних моделі чи ні. Дослідники змогли передбачити основну процедуру пацієнта (наприклад, операцію, яку пацієнт переніс) на основі атрибутів (наприклад: вік, стать, лікарня) [1].

Пом’якшення:

- Використання випадання нейронів і стекування моделей може бути певною мірою ефективним пом’якшенням наслідків. Використання відсіву нейронів не тільки підвищує стійкість нейронної мережі до цієї атаки, але й підвищує продуктивність моделі [4].

Висновки та перспективи. Отже, можна дійти до висновку, що найбільшою загрозою безпеці в машинному навчанні сьогодні є отруєння даних через відсутність стандартних засобів виявлення та пом’якшення в цьому просторі , у поєднанні із залежністю від недовірених, або неконтрольованих

загальнодоступних наборів даних як джерел навчальних даних. Для зменшення впливу атак зловмисників слід використовувати запропоновані пом'якшення для сховищ навчальних даних та систем на яких вони розміщені.

Список використаних джерел:

1. Ram Shankar Siva Kumar, David O'Brien, Kendra Albert, Salome Viljoen, Jeffrey Snover. Failure Modes in Machine Learning, [Електронний ресурс] – Режим доступу: https://arxiv.org/ftp/arxiv/papers/1911/1911.11034.pdf
2. Wenqi Wei, Ling Liu, Stacey Truex, Lei Yu, Mehmet Emre Gursoy, Yanzhao Wu. Adversarial Examples in Deep Learning:Characterization and Divergence: arXiv:1807.00051v3 [cs.LG], [Електронний ресурс] – Режим доступу: https://arxiv.org/pdf/1807.00051.pdf
3. Xi Wu, Uyeong Jang, Jiefeng Chen, Lingjiao Chen, Somesh Jha. Reinforcing Adversarial Robustness using Model Confidence Induced by Adversarial Training, [Електронний ресурс] – Режим доступу: http://proceedings.mlr.press/v80/wu18e/wu18e.pdf
4. Ahmed Salem, Yang Zhang, Mathias Humbert, Pascal Berrang, Mario Fritz, Michael Backes. ML-Leaks: Model and Data Independent Membership Inference Attacks and Defenses on Machine Learning Models: arXiv:1806.01246v2 [cs.CR], [Електронний ресурс] – Режим доступу: https://arxiv.org/pdf/1806.01246v2.pdf

Мутьянов Володимир Михайлович
Навчально-науковий інститут Інформаційних технологій
Державний університет телекомунікацій м. Київ

ЗАСТОСУВАННЯ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ГАЛУЗІ ЕКОЛОГІЇ

Комп'ютерні інформаційні технології – це потужний інструмент збору, аналізу та зберігання даних в будь-якій сфері промисловості та науки, що потребує цього. Здатність інформаційних систем вести пошук у базах даних, приєднувати власні бази, здійснювати просторові запити, безперервно накопичувати та коригувати наявні просторові й часові дані, моделювати та відтворювати реальні ситуації, заощадити час і кошти державних та комерційних структур, унеможливити виникнення кризових та аварійних ситуацій.

Екологічна інформаційна система (ЕІС) – це система керування екологічною інформацією, її аналізу та подання з метою ефективного прикладного застосування за мінімальних фінансових витрат. Екологічну інформацію можна подати у вигляді набору даних, що моделюють навколишнє середовище, за допомогою узагальнених структур даних.

При розробці нових пристроїв, дослідженні невивчених або невідомих явищ та процесів, побудові систем розпізнавання, що мають задані характеристики інформаційного сигналу або невідомі характеристики, які підлягають вивченню, комп'ютерне моделювання та аналіз дозволяє створити математичні моделі об'єкта, що розробляється чи вивчається. Такий підхід вимагає істотно менших витрат часу та технічних засобів порівняно з фізичним експериментом, особливо на попередній стадії розробки, за відсутності достовірної заздалегідь відомої інформації про навколишнє середовище та об`єкти, що в ньому перебувають.

Основним завданням екологічного моніторингу є забезпечення системи

керування природоохоронної діяльності та екологічної безпеки своєчасною і точною інформацією, що дає оцінку стану навколишнього середовища, дозволяє спеціалістам виявити причини та можливі наслідки змін його стану, а також визначити необхідні захисні дії. За функціональним призначенням виділяють три види моніторингу навколишнього середовища: стандартний, кризовий, науковий.

В екоінформаційній системі можна виділити три рівні, орієнтовані на розв'язання різних задач екологічного моніторингу, які різняться методами роботи з екологічною інформацією. Верхній рівень складається з програмних модулів підтримки прийняття рішень, середній – програмне забезпечення системного аналізу інформації про стан навколишнього середовища, нижній – модулі опрацювання первинної екологічної інформації. На нижньому рівні використовуються різні системи управління базами даних (СУБД) типу Oracle чи Microsoft SQL Server для зберігання даних про стан навколишнього середовища, а для опрацювання результатів спостережень застосовують електронні таблиці, пакети прикладних програм типу MathCAD, Surfer та інші. Із прогресивним розвитком технологій програмування типу Silverlight, Flash, JAX та мов програмування C++ , C#, Java, Delphi, Turbo-Prolog, Lisp стало можливо використовувати мережу Internet для миттєвого доступу до екоданих та їх візуалізації з будь-якої точки планети, що має доступ до мережі.

Потрібно зазначити, що найбільшого розвитку інформаційні технології досягли в США. Мапи, створені комп'ютерами та розміщені на веб-сайті КТСД (Коаліція щодо токсикантів Силіконової Долини) - один з прикладів того, як інформаційні технології розширюють можливості моніторингу довкілля. Супутникові технології надають нам картину змін в довкіллі досі не баченої чіткості. Серед багатьох таких картин - поширення пожеж у тропічних лісах південно-східної Африки, втрата озону над Антарктикою, зменшення розмірів та обміління Аральського моря. Сьогодні все більше супутників знімають такі картини людської діяльності на Землі.

Досить активно в цьому напрямі працює і Європейське космічне агентство (ЄКА). Прикладом цього є проект "Глобальний моніторинг навколишнього середовища та безпеки". Зростаючий потік супутникових даних дає цінну інформацію, зокрема, для управління природокористуванням, оцінки наслідків природних та техногенних катастроф і розподілу гуманітарної допомоги. Слід згадати і сумісний проект ЮНЕСКО й ЄКА щодо порятунку об'єктів, які включені у список Всесвітнього культурного спадку, в межах якого здійснюється безперервний моніторинг різноманітних архітектурних та природних пам'ятників, а також національних парків і місць існування рідкісних та зникаючих видів тварин та рослин.

Програмне забезпечення ГІС (географічна інформаційна система) дає змогу зберігати, аналізувати і вправно користуватися даними, отриманими з супутників. Ця інформація разом з наземними спостереженнями та іншими даними може допомагати дослідникам вивчати забруднення та інші екологічні небезпеки, знаходити багаті на окремі ресурси регіони і моделювати зміни у довкіллі. Це також може допомогти тим, хто планує і приймає рішення, краще будувати наші стосунки з довкіллям. До того ж, дослідники використовують

комп'ютери для вивчення різних екологічних сценаріїв - від альтернативних транспортних засобів для міських перевезень до спалювання викопного палива по всьому світу.

Для прикладу, сьогодні уже створені бази даних географічної ІС (ГІС). Так в програмному забезпеченні ESRI® ArcGIS® ці три види баз даних подані каталогом (ГІС як колекція наборів геоданих), картою (ГІС як інтелектуальний картографічний вид) і набором інструментів (ГІС як набір інструментів для інтелектуальної обробки просторових даних). Всі вони є невід'ємними складовими повноцінної ГІС і більшою чи меншою мірою використовуються у всіх ГІС-додатках.

Список використаних джерел:

1. *В. М. Заяць// Підходи до побудови екоінфомаційних систем на основі інформаційно-комп`ютерних технологій*
2. *Заверуха Н.М., Серебряков В.В., Скиба Ю.А. Основи екології*

Дзицюк Андрій Олександрович,
студент 5 курсу, групи КСДМ-51
(050)-595-09-92
andrey.dzitsuk@gmail.com
Науковий керівник: Ткаченко Ольга Миколаївна,
доктор технічних наук,
завідуюча кафедрою Комп’ютерної інженерії
Державного університету телекомунікацій, м. Київ

РЕЗЕРВУВАННЯ КРИТИЧНИХ МЕРЕЖЕВИХ ВУЗЛІВ В КОМП’ЮТЕРНИХ МЕРЕЖАХ

1. Постановка задачі.Ознайомити слухачів із необхідністю забезпечення резервування мережевих вузлів у комп’ютерних мережах.
2. Мета дослідження. Донести інформацію по темі, розділивши її на 3 пункти:
   1) Що таке резервування?
   2) Проблеми використання протоколу OSPF
   3) Переваги та недоліки резервування вузлів за допомогою протоколу OSPF
3. Результати дослідження.
   1) Резервування — протокол резервування мережевих ресурсів. Розглянемо на прикладі протокол OSPF, працює він таким чином: Коли OSPF налаштований, він прослуховує своїх сусідів по мережах і збирає всі наявні дані про стан зв'язку. Ці дані потім використовуються для складання топологічної карти, яка містить усі доступні шляхи в мережі. Ця база даних зберігається для використання, і ми називаємо її база даних державних посилань. Після створення бази даних посилань його використовують для обчислення

найкоротшого шляху до підмереж / мереж за допомогою алгоритму, відомого як “Open Shortest Path First”, який був розроблений Edsger W Dijkstra.

2) До основних проблем OSPF можна віднести роботу протоколу в мережах з множинним доступом. Поширена топологія, при якій безліч маршрутизаторів об'єднуються не через послідовне підключення один до одного, а через загальну мережу. Теоретично OSPF повинен вибудовувати сусідства в межах загальної мережі на основі принципу «кожен з кожним». Однак це вимагає формування величезних таблиць, робота з якими сильно перевантажує процесор і пам'ять.

Вирішення цієї проблеми досягається за допомогою механізму вибору Designated Router (DR) і Backup Designated Router (BDR), які представляють собою ролі маршрутизаторів. У мережі з множинним доступом, до якої підключені більше 2 маршрутизаторів, один з них призначається на роль DR, а другий — на роль BDR. При відправці будь-яким маршрутизатором будь-якого пакета, він надходить не всім пристрою в мережі, а подається на окремий мультикастовий адресу, доступний тільки DR і BDR. У свою чергу, DR розсилає пакет всім маршрутизаторам в мережі. Таке посередництво значно знижує навантаження. BDR виконує резервну функцію і моментально приймає роль DR при його відключенні. Після цього серед інших маршрутизаторів відразу вибирається новий BDR.

3) Переваги OSPF:

- OSPF легко масштабується, тобто з дуже невеликою кількістю клопоту, ми можемо масштабувати його для використання у дуже великій мережі
- Перший протокол відкритого найкоротшого шляху має повну підтримку підмереж.
- Використання привітних пакетів: OSPF надсилає невеликі привітні пакети для перевірки операцій зв'язку та ігнорує передачу великих таблиць.
- OSPF підтримує тегування маршрутів: У OSPF маршрути можна позначати, щоб полегшити взаємодію з довільними значеннями.
- Маршрутизація: OSPF може маршрутизувати пакети залежно від їх типу службового поля.

Недоліки OSPF:

- OSPF - це інтенсивно використовуваний процесор протокол.
- Оскільки в ньому зберігається більше однієї копії інформації про маршрутизацію, вона споживає більше пам’яті.
- OSPF - це більш складний протокол для розуміння та вивчення в порівнянні з іншими Інтернет-протоколами.

Висновки та перспективи

Open Shortest Path First (OSPF) - як протокол маршрутизації займає важливе місце в інтернет-інфраструктурі. Бути в змозі легко та швидко знайти найкоротший шлях допомагає зменшити непотрібне навантаження на мережу, а можливість знайти інший шлях у разі помилки на оптимальному допомагає підвищити стабільність мережі.

Список використаних джерел
1. Бачинский В.А., Гіоргізова-Гай В.Ш., Вибір протоколу динамічної маршрутизації в корпоративній IP-мережі // Системні дослідження та інформаційні технології, №1, 2015 – 100с.
2. Керівництво з управління OSPF, Cisco [електронний ресурс] - www.cisco.com/c/ru_ru/support/docs/ip/open-shortest-path-first-ospf/7039- 1.pdf
3. Enhanced Interior Gateway Routing Protocol // Cisco [електронний ресурс] - http://docwiki.cisco.com/wiki/Enhanced_Interior_Gateway_Routing_Protoc ol

Куц Данило Сергійович,
студент 5 курсу, групи КСДМ-51
Державного університету телекомунікацій
danielzet14@gmail.com
Державного університету телекомунікацій, м. Київ

БАГАТОКАНАЛЬНИЙ ЗВ'ЯЗОК ЯК ВАРІАНТ ЗБІЛЬШЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ І МЕРЕЖ

1.1 Сучасні тенденції розвитку багатоканальних телекомунікаційних систем

Сучасні тенденції розвитку багатоканальних телекомунікаційних систем пов'язані з підвищенням їх пропускної спроможності, покращенням їх надійності та економічності, що досягається подальшим ускладненням процесів інформаційного обміну, що протікають. Ускладнення процесів інформаційного обміну пов'язане з постійним збільшенням кількості паралельно функціонуючих каналів, додаткових підсистем передачі повідомлень, розвитком нових інформаційних технологій підтримки передачі повідомлень.

Збільшений обсяг інформації, що генерується сучасним суспільством, вимагає нових підходів щодо обробки та передачі інформації у телекомунікаційних системах та мережах. Одним із способів збільшення пропускної спроможності телекомунікаційних систем та мереж є використання принципу багатоканального зв'язку. Суть багатоканальності полягає у передачі великої кількості повідомлень від різних джерел інформації із загальної лінії зв'язку.

1.2 Досягнення нових показників ефективності

З метою досягнення нових якісних показників ефективності в діючих багатоканальних системах необхідно забезпечити узгоджену інтеграцію всіх процесів інформаційного обміну через постійну зміну умов експлуатації, викликаних локально-просторовою та тимчасовою зміною трафіку, виду та характеру шумової обстановки в зоні обслуговування, випадковими змінами параметрів каналів зв'язку.

Багатоканальність передачі повідомлень забезпечується за допомогою використання методів сигнального ущільнення: частотного, тимчасового, кодового та ін. параметрів середовища розповсюдження сигналів тощо. При

цьому також виникає необхідність збільшення пропускної спроможності вже діючих телекомунікаційних систем, що експлуатуються, до яких, зокрема, можна віднести системи теле і радіомовлення. Це завдання можна вирішити за допомогою застосування альтернативних методів канального ущільнення, до яких можна віднести ущільнення гомогенних сигналів на основі вторинного використання широкосмугових каналів (яке також називатимемо вторинним ущільненням).

Основна особливість ущільнення гомогенних сигналів (вторинного ущільнення) полягає в тому, що ущільнюванні сигнали багатоканальної телекомунікаційної системи мають спектрально-часові характеристики, що взаємно перетинаються. При цьому ущільнюванні сигнали можна порівняти по ширині спектрів, корелювати з стаціонарними. Слід зазначити, що можливість ущільнення гомогенних сигналів обумовлюється тим, що багато широкосмугових сигналів (особливо аудіо-, відеосигнали) близькі за своєю природою, характеризуються значною інформаційною надмірністю і допускають певний рівень втрати інформації, при якій ця втрата практично не відчувається людиною.

1.3 Можливі проблеми пов’язані з впровадженням

Серед них можна виділити складності, пов'язані з взаємним спотворенням ущільнюванних сигналів через накладання один на одного їх спектрально-часових характеристик, труднощі забезпечення лінійної незалежності ущільнюванних сигналів з метою їх виділення на приймальній стороні, відсутністю ефективних методів та алгоритмів синтезу частотних та часових характеристик ущільнюванних сигналів. Слід також зазначити, що відомі методи вторинного ущільнення не повною мірою враховують особливості сприйняття людиною інформації, що надходить, що зменшує ефективність цих методів і робить актуальним завдання розробки методів і алгоритмів вторинного ущільнення гомогенних сигналів з спектрально-тимчасовими характеристиками.

ВИСНОВКИ

В ході дослідження було запропоновано метод збільшення пропускної здатності телекомунікаційних систем. Розглянуто наявні методики та можливості їх впровадження. Виявлено можливі проблеми пов’язані з їх застосуванням.

Багатоканальний зв’язок у телекомунікаційній сфері є акутальною темою для дослідження, так як обсяг інформації буде тільки зростати, а можливості устаткування не безграничні.

Список використаних джерел

1. ITU-R Recommendation BT.653-3: Teletext systems. 1998. 21 p.
2. Лев О.Ю. Теоретичні засади багатоканального зв'язку. Підручник для електротехн. ін-тів зв'язку. М., "Зв'язок", 1978. 192 с.
3. Красильників Н.Н. Теорія передачі та сприйняття зображень. М. «Радіо та зв'язок», 1986. 248 с.
4. Янушевський Р.Т. Теорія лінійних оптимальних багатозв'язкових систем управління. - М: Наука, 1973. 464 с.

Медвецький Володимир Юрійович
студент 5 курсу, групи КСДМ-51
(099) 709 39 06
medvetsky_vladimir@ukr.net
Державного університету телекомунікацій м. Київ

ПРОБЛЕМАТИКА ОРГАНІЗАЦІЇ ЗАХИЩЕНИХ СЕРВЕРНИХ ПРИМІЩЕНЬ

Серверне приміщення за правом можна назвати «серцем» офісних будівель. У цьому приміщенні сконцентровано обладнання, без якого вже важко уявити сучасний офіс. Тут розташовуються комутаційні стійки, серверне обладнання, джерела безперебійного живлення обладнання і т.д. Загалом, можна констатувати, що серверна - це приміщення спеціального призначення, в якому розташовується телекомунікаційне обладнання та до якого висувається ряд певних вимог. Про організацію серверного приміщення ми сьогодні і поговоримо.

Постановка задачі. Відразу варто зазначити, що організація серверного приміщення - процес не дешевий і до нього потрібно підходити з чітким розумінням того, навіщо нам потрібно проектувати серверну. Виходячи з цього, ми можемо зрозуміти, який тип приміщення і його розміри нам потрібні. Чи достатньо однієї кімнати, для централізованого встановлення обладнання або краще його рознести по невеликим настінним шафам по всьому офісу? Все залежить від поставленої задачі, від розмірів, від конфігурації самого офісу.

Мета дослідження. Важко собі уявити сучасну організацію, в якій би була відсутня серверна IT-система. Будучи ключовою ланкою IT-інфраструктури, сервер являє собою дорогу і в той же час найбільш вразливу частину всього комплексу обчислювального і телекомунікаційного обладнання. Вона завжди була головним об'єктом вірусних атак та спроб несанкціонованого доступу до системи, тому особливу увагу треба приділити захисту серверного приміщення від цих загроз. При цьому до недавнього часу не приділялося належної уваги до не менш важливих причин збоїв: несприятливих умов навколишнього середовища, наприклад, протікання води з верхнього поверху, а також змін фізичних параметрів обладнання.

Результати дослідження. Як показує практика, фактори, пов'язані з фізичним доступом до апаратного обладнання, перебоями в електроживленні, зміною температурного режиму і вологості повітря, а також вібрацією, електромагнітними перешкодами грають ключову роль в підтримці високого рівня продуктивності та ефективності мережі. Незначні, на перший погляд, відхилення цих показників можуть спричинити не тільки збої в роботі програмного забезпечення, але також часті пошкодження і навіть втрату дорогого обладнання.

Очевидно, що збереження цих параметрів в межах норми, багато в чому визначає рівень захисту інформації, безперервність робочих процесів і надійність роботи обладнання всієї IT-системи.

Більшість організацій, що використовують інформаційні системи, розташовують їх в приміщеннях, часто не призначених для цих цілей, що, звісно,

не може не відображатися на роботі серверного обладнання. Чим функціональніше і точніше IT-система, тим примхливішою і чутливішою вона стає до впливу негативних зовнішніх чинників. Це, перш за все, відноситься до серверів, які
підтримують життєдіяльність всієї мережі.

Висновки та перспективи. Найбільш ефективним методом вирішення цієї проблеми є використання комплексного підходу до створення, так званих, захищених серверних приміщень. Спеціальне обладнання, що розташоване в таких приміщеннях, створює штучні умови для оптимальної роботи обладнання, що знаходиться в серверній, а також обмежує фізичний доступ до приміщення. Але до прийняття такого рішення організація повинна «дорости», оскільки воно вимагає значних фінансових вкладень. Рішення про спеціальне обладнання захищеного серверного приміщення для «серця IT-системи» приймають підприємства, які усвідомили необхідність в оптимізації своєї інформаційної інфраструктури, підвищенні ефективності, надійності і керованості систем, а також у зниженні загальної вартості їх володіння.

Список використаних джерел:

1. *Інтернет-джерело: http://studentam.net.ua/content/view/7557/97/*
2. *Д. Матат // Освіта України*
3. *Building a modern data center - Principles and strategies of design written by Scott D. Lowe, James Green and David Davis - Focus on Customer Service and the Business – 19 p.*

В’юннік Юрій Олександрович
студент 5 курсу, групи КСДМ-51
(050) 295 59 20
shelkanin09@gmail.com
Державного університету телекомунікацій, м. Київ

ПЕРЕВАГИ ВИКОРИСТАННЯ VPN МЕРЕЖ

На жаль, з'єднання через Інтернет не настільки безпечне, як через виділені лінії або мережі на базі служб мережі WAN. Використовуючи можливості Інтернету, зловмисник може знайти прості способи отримання бажаних копій пакетів даних. Для цього навіть не потрібно відходити від комп'ютера. Віртуальні приватні мережі (Virtual Private Network - VPN) надають оптимальне рішення проблем безпеки, які виникають при використанні відкритого Інтернету в якості приватної служби мережі WAN

Мета використання. Мета даної технології полягає в забезпеченні відокремлення потоку трафіку одного приватного підприємства від глобальної мережі Інтернет. Таким чином ця технологія забезпечує захист конфеденційних даних в мережах загального користування від несанкціонованого доступу.

Однією із найголовніших функцій ВПН технології є надання надійного рівня криптографії. В ній має бути налаштоване шифрування інформації, відповідна аутентифікація для доступу, засоби захисту від можливого

проникнення із загальної мережі. Такі можливості технології можуть гарантувати кінцевому користувачеві захист його корпоративних даних та конфіденційних файлів.

Засоби шифрування. Перед шифруванням даних використується механізм протоколу обміну ключами. Який можна представити у вигляді двох фаз.

На першому етапі. Учасники мають аутинтифікувати один іншого у мережі і домовитися о параметрах шифрування під час з‘єднання у мережі. Параметри цього тунеля визначаються політикою ISAKMP до режиму редактування якої можна потрапити завдяки команді crypto isakmp policy номер_політики. Якщо учасники домовилися о параметрах , то створюється відповідний тунель ISAKMP і процес переходить до другої фази.

На другому етапі, після налагодження довірчих відносин, учасники домовляються о побудові тунелю для передачі даних. Пропонуючи один одному варіанти побудови, вказані у команді crypto ipsec transform-set. І після того, як 32 доходять згоди підміється основний тунель. В якому і відбувається шифрування даних. Шифрування даних відбувається за чотири основні етапи.

На першому етапі. Пристрій-відправник в мережі VPN підставляє вихідні дані і ключ шифрування в формулу, до якої прозводиться шифрування.

На другому етапі. Пристрій-відправник інкапсулює зашифровані дані в пакет з новим заголовком IP і заголовком VPN.

На третьому етапі. Пристрій-відправник пересилає цей пакет пристроюотримувачу в мережі VPN.

На четвертому етапі. Пристрій-отримувач в мережі VPN розшифровує пакет, завдяки спеціальній заданній формулі. У неї доставляются зашифровані дані і ключ шифрування, значення якого співпадає з тим, яке використовувалось в пристрої-відправнику мережі VPN.

Висновки та перспективи. Ви рятуєтеся від незахищених критичних точок: ваша інформація розміщується ізольовано в загальному сховищі з єдиною точкою входу. Час - гроші, і мова не тільки про зручність, але і про ефективність. Ви не просто економите час, але і підвищуєте гнучкість ваших послуг, надаючи клієнтам можливість віддаленого взаємодії з вами. Ваші співробітники і клієнти можуть з'єднуватися з вашою мережею, не побоюючись того, що їх інформація потрапить в сторонні руки завдяки шифруванню данних.

Список використаних джерел:

1. Комп'ютерні мережі та телекомунікації : навч. посібник / В. А. Ткаченко, О. В. Касілов, В. А. Рябик. – Харків: НТУ "ХПІ", 2011. – 224 с.
2. *Буров Є. В. Комп'ютерні мережі: підручник / Євген Вікторович Буров. — Львів: «Магнолія 2006», 2010. — 262 с. ISBN 966-8340-69-8*
3. *Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. — Львів: «Магнолія 2006», 2013ю — 256 с. ISBN 978-617-574-087-3.*

Котубей Назар Іванович
Студент 5 курсу, крупи КСДМ-51
Державного університету телекомунікацій
(095)6949731
nazar.kotubey@gmail.com
Науковий керівник: Ткаченко Ольга Миколаївна,
доктор технічних наук, професор,
завідуюча кафедрою Комп'ютерної інженерії
Державного університету телекомунікацій, м. Київ

МЕТОДИ ТЕСТУВАННЯ ПРОДУКТИВНОСТІ КОМП'ЮТЕРНИХ СИСТЕМ

Тестування продуктивності (performance testing) в програмній інженерії – це тестування, яке проводиться з ціллю визначення, як швидко працює програма або її частина під деяким навантаженням. Також може служити для перевірки та підтвердження інших атрибутів якості системи, таких як масштабованість, надійність та споживання ресурсів. Це одна зі сфер діяльності інженерії продуктивності, що розвивається та яка прагне враховувати продуктивність на стадії моделювання та проектування системи, перед початком основної стадії кодування.

Постановка задачі. Дана публікація має на меті продемонструвати актуальні методи тестування продуктивності комп'ютерних систем, а також дослідити їх принципи роботи та порівняти відмінності підходів до вирішення різних задач.

Мета дослідження. Аналіз напрямків у тестуванні продуктивності: навантажувальний (load), стрес (stress), тестування стабільності (endurance, soak, stability), конфігураційне (configuration). Дослідження підходів до тестування продуктивності програмного забезпечення:

- у термінах робочого навантаження: програмне забезпечення піддається тестуванню у ситуаціях, що відповідають різним сценаріям використання;
- у межах бета-тестування, коли система випробовується реальними кінцевими користувачами.

Навантажувальне тестування – це найпростіша форма тестування продуктивності. Навантажувальне тестування зазвичай проводиться для того, щоб оцінити поведінку програми під заданим очікуваним навантаженням. Цим навантаженням може бути, наприклад, очікувана кількість одночасно працюючих користувачів програми, що здійснюють задану кількість транзакцій за інтервал часу. Такий тип тестування зазвичай дозволяє отримати час відгуку всіх найважливіших бізнес-транзакцій. У разі спостереження за базою даних, сервером додатків, мережею і т. д. цей тип тестування може також ідентифікувати деякі вузькі місця програми.

Результати дослідження. Стрес-тестування зазвичай використовується для розуміння меж пропускної спроможності програми. Цей тип тестування проводиться для визначення надійності системи під час екстремальних або диспропорційних навантажень і відповідає на питання про достатню продуктивність системи у випадку, якщо поточне навантаження перевищить

очікуваний максимум.

Тестування стабільності проводиться з метою переконатися в тому, що програма витримує очікуване навантаження протягом тривалого часу. Під час проведення цього виду тестування здійснюється спостереження споживанням додатком пам'яті, щоб виявити потенційні витоки. Крім того, таке тестування виявляє деградацію продуктивності, що виражається у зниженні швидкості обробки інформації та/або збільшенні часу відповіді програми після тривалої роботи порівняно з початком тесту.

Конфігураційне тестування - ще один із видів традиційного тестування продуктивності. У цьому випадку замість того, щоб тестувати продуктивність системи з точки зору навантаження, тестується ефект впливу на продуктивність змін в конфігурації. Хорошим прикладом такого тестування може бути експерименти з різними методами балансування навантаження. Конфігураційне тестування також може бути поєднане з навантаженням, стресом або тестуванням стабільності.

Висновки та перспективи. Отже, для комплексної оцінки продуктивності системи потрібно використовувати тестування різними вищезазначеними методами, щоб зрозуміти відносну продуктивність системи. Таким чином можна отримати цілісну загальну картину продуктивності того, чи іншого технічного рішення.

Список використаних джерел:

1. *Інтернет-джерело:https://hi-news.pp.ua/tehnka-tehnologyi/9094-shvidka-perevrka-produktivnost-kompyutera.html*
2. *IEEE Guide to Software Engineering Body of Knowledge, SWEBOK, 2004*
3. *Інтернет-джерело: http://pro-computer.pp.ua/8834-test-procesora-kompyuterna-dagnostika.html*

Машлянка Д.В.,
Студент групи ПД-42
Науковий керівник: Коба А.Б.
Старший викладач кафедри інженерії програмного забезпечення
Навчально-науковий інститут інформаційних технологій
Державного університету телекомунікацій, м. Київ

АКТУАЛЬНІСТЬ ЧАТ-БОТУ У СФЕРІ БІЗНЕСУ

У сучасному світі бізнес-організації різних форм власності часто зустрічаються з диверсифікованими проблемами, зокрема, з понаднормовими витратами, недостатньою підтримкою, супроводом клієнтів та зменшенням ефективності діяльності тощо.

Для того, щоб покращити надання послуг та у свою чергу зробити підприємство економічно прогресивним, конкурентоспроможним не достатньо покращити виробничі процеси, а потрібно зробити новий крок для розвитку бізнесу, залучити та інтегрувати у власні бізнес-процеси дієві цифрові

маркетингові інструменти.

Одне з найбільш поширених питань у бізнесі – обслуговування клієнтів. Чатботи у цьому випадку допомагають не лише скоротити витрати, але також збільшити точність даних та зменшити затримку у відповіді клієнту на його запит. Згідно з даними американського журналу Forbes, 80% маркетологів планують використовувати чат-боти у своїх бізнес-процесах вже у 2021 році, що підтверджує актуальність даного цифрового інструменту. Тому, можна впевнено спрогнозувати, що в майбутньому чатботи витіснять звиклі інструменти, телефонні розмови та e-mail-листування.

На разі, основною проблемою введення чат-боту бізнесом є недовіра клієнтів до даного інструменту, адже вітчизняне суспільство все ще надає перевагу людському ресурсу понад штучним інтелектом. І хоча ця технологія ще не скоро зможе замінити електронну пошту та телефонний зв'язок повністю, оскільки деякі питання потребують людського втручання, чат-боти є технологією, яка допомагає подолати «вузькі місця» у каналах комунікації та покращити роботу організації.

Щоб створити ефективний чат-бот потрібно визначити бізнес-вимоги компанії, зрозуміти основні та допоміжні бізнес-процеси. Він має не лише їм відповідати, але й вирішувати поставлену проблему. Не менш важливим є вибір правильної платформи для реалізації та інтегрування чат-боту. Інтерфейс повинен бути зрозумілим для клієнтів, а платформа бути надійною з точки зору інфраструктурного забезпечення.

Боти зі штучним інтелектом стали необхідною частиною маркетингової стратегії, що допомагає раціонально налагодити комунікаційну складову бізнесу, забезпечити взаємодію із цільовою аудиторією 24/7. В найближчому майбутньому, за допомогою штучного інтелекту, боти будуть більш вдосконалені, а люди в свою чергу знайдуть інші способи для їхнього використання і застосування не лише у бізнесі, але і у всіх сферах життя. Таким чином, можна впевнено стверджувати, що технологія чатботів радикально трансформує методи взаємодії бізнесу з клієнтами.

Список використаних джерел:

1. Oracle Cloud Infrastructure (OCI) application development services.[Електронний ресурс] – Ресурс доступу: https://www.oracle.com/chatbots/what-is-a-chatbot/.
2. What are the Benefits of Chatbot for your Business?.[Електронний ресурс] – Ресурс доступу: https://marutitech.com/benefits-chatbot/ .

Бортнік Василь Олегович,
Студент 5 курсу, групи КСДМ-51
(068)-050-71-13
bortnsk00@gmail.com
Науковий керівник: Ткаченко Ольга Миколаївна,
Кандидат технічних наук,
Завідуюча кафедри Комп'ютерної інженерії
Державного університету телекомунікацій, м. Київ

РІВНІ ДЕТАЛІЗАЦІЇ ПРИ ВІЗУАЛІЗАЦІЇ В РЕАЛЬНОМУ ЧАСІ

Постановка задачі. Ознайомити слухачів із поняттям рівнів деталізації та їх застосуванням у realtime rendering.

Мета дослідження. Донести інформацію про рівні деталізації та їх застосування: 1. Що таке рівні деталізації?
2. Необхідність автоматизування даного процесу.
3. Алгоритми для спрощення сітки.

Результати дослідження. Спочатку, варто розібратися із поняттям рівнів деталізації або ж LOD (Level of detail з англ.).

У комп'ютерній графіці поняття рівень деталізації або LOD відноситься до складності представлення сітки точок тривимірної моделі[1]. LOD є комплексним та абстрактним поняттям, представленим вже великий час у світі програмного забезпечення для створення комп'ютерні графіки, але воно залишається актуальним й досі. Суть його полягає в тому що рівень деталізації можна зменшити за деяких умов і така зміна залишеться незаміченою для людського ока. До таких умов можуть відноситися: відстань до об'єкта, його відносна швидкість на екрані, розмір об'єкта на екрані, а також наприклад LOD може активно налаштовуватись в залежності від показників роботи системи. Більшість часу LOD застосовується до геометрії об'єктів, але також існують алгоритми для спрощення текстурних об'єктів на етапі візуалізації графічного конвеєру. Форма управління рівнем деталізації застосовувалася до текстурних карт протягом багатьох років під назвою mipmapping , що також забезпечує вищу якість візуалізації[1].

Впровадження різних рівнів деталізації в першу чергу орієнтоване на забезпечення високої оптимізації та продуктивності системи, адже в сучасних ком'ютерних іграх, симуляторах, програмах для геолокації і т.д. необхідно забезпечувати швидку візуалізацію зображення (у деяких випадках до 144 кадрів за секунду або ж 6.9 мс на кадр). Спостерігаючи у віртуальному просторі шедеври архітектури вдалині, неможливо одразу оцінити та роздивитись різані колони, недоліки каміння з якого його побудували або ж найдрібніші деталі орнаменту, що прикрашає фасад[2]. Особливо це стосується віртуального середовища. Тут варто задати риторичне питання: «Навіщо витрачати продуктивність GPU на візуалізацію високо полігонального об'єкта, якщо ми все одно обмежені тим, що розрізняє наш біологічний інструмент?».

Найкращий підхід до цього питання впровадження автоматичного спрощення моделі. Таким чином спочатку необхідно підготувати високо деталізовану модель, з великою кількістю полігонів в геометричній сітці та

текстурами високого розширення. Далі або вручну, або за допомогою спеціальних програм, або ж алгоритмів підготувати декілька моделей для різних відстаней, де найгірша за якістю модель відповідатиме найбільшій відстані або найгіршим показникам продуктивності комп'ютерної системи.

Багато готових рішень у вигляді "Game engine" йдуть зі своїм готовим набором алгоритмів для автоматичної генерації різних рівнів деталізації, серед таких наприклад: UNIGINE, Unreal Engine, Unity та Blender. Вони дозволяють змінювати параметри використання LOD в приємному та доступному графічному інтерфейсу, що дозволяє значно зменшити час на розробку та підготовку моделей. При роботі із власним продуктом варто звернути увагу на алгоритми спрощення та ускладнення геометричної сітки об'єктів. Такі алгоритми використовуються в графічних API, таких як: DirectX, OpenGL та CUDA. Серед цих алгоритмів:

- «Real–time Mesh Simplification Using GPU»[3];
- «Parallel mesh decimation with GPU»[4];
- «CPU–GPU algorithms for triangular surface mesh simplification»[5].

Впровадження цих алгоритмів дозволяє значно прискорити візуалізацію та растеризацію сцени, має абсолютний контроль над тим як та що буде відбуватись, проте потребує значних знань та вмінь від інженера комп'ютерної графіки. Останній варіант це підготовка різних LOD художниками. При такому підході дану частину роботи можна віддати на outsource, що дозволить зменшити завантаженість команди розробників, однак потребуватиме збільшення фінансування проекту.

Висновки та перспективи. Отож, можна сказати, що впровадження LOD буде актуальним завжди, адже зі збільшенням продуктивності комп'ютерних систем, збільшуються вимоги до програм, що знову призводить до потреби в оптимізації. На даний час неможливо у режимі реального часу відтворювати тисячі об'єктів, що складаються із мільйонів полігонів, тому зберігається гостра необхідність у використанні LOD. Описані підходи до впровадження та розробки різних рівнів деталізації є гнучкими та їх можна застосовувати на різних проектах відповідно до потреб та можливостей.

До перспектив, варто віднести покращення існуючих алгоритмів для об'єктів із скелетом (*Skinned Mesh*), так як поєднання двох алгоритмів може призвести до небажаних графічних результатів[2].

Список використаних джерел:

1. Level of detail (computer graphics) [Електронний ресурс] – Режим доступу до ресурсу:https://en.wikipedia.org/wiki/Level_of_detail_(computer_graphics)#Rendering_and_modeling_software
2. Автоматична генерація рівнів деталізації: must-have для realtime-візуалізації: https://habr.com/ru/company/unigine/blog/666770/
3. DeCoro C., Tatarchuk N. "Real–time Mesh Simplification Using GPU" in Proceedings of the symposium on interactive 3D graphics and games, 2007.
4. Vad'ura J. "Parallel mesh decimation with GPU" 2011.
5. Shontz S., Nistor D. "CPU–GPU algorithms for triangular surface mesh simplification" in Proceedings of the 21st international meshing roundtable, pp. 475–492, Springer, Berlin, 2013.

Трудов Антон Денисович
Студент 5 курсу, групи КСДМ-51
Державний університет телекомунікацій, м. Київ
Навчально-науковий інститут інформаційних технологій
(063)-724-22-75
trudovanton1@gmail.com
Науковий керівник: Ткаченко Ольга Миколаївна,
Кандидат технічних наук,
Завідуюча кафедри Комп'ютерної інженерії
Державного університету телекомунікацій, м. Київ

ПЕРСПЕКТИВА РОЗВИТКУ 6G

З моменту своєї першої комерціалізації на початку 2019 року 5G прогресує у всьому світі та проникає в повсякденне життя. Тепер інтерес дослідників до бездротового зв'язку швидко переміщається на мобільну систему наступного покоління — 6G.

Постановка задачі. Ознайомити слухачів із перспективами розвитку шостого покоління мобільного зв'язку.

Метою дослідження. Донести інформацію про сценарії та варіанти використання 6G, найсучасніші технології та заходи стандартизації.

Результати дослідження. Більшість попередніх дописів описували 6G з точки зору взаємодії між фізичним світом, цифровим світом та біологічним (людським) світом, особливо наголошуючи на інтеграції кібер- та фізичного простору в реальному часі. На основі цих попередніх внесків ми концептуалізуємо 6G як трикутник, де три вершинні точки представлені кіберпростором, фізичним простором і зв'язком із внутрішнім ядром, що представляє інтелект.

Повністю інтегрований кіберпростір і фізичний простір стануть новою платформою Інтернет для надання різних видів вертикалей 6G, включаючи додатки на основі метавсесвіту або кібер-фізичної системи (CPS). Зв'язок, що забезпечується майбутніми передовими комунікаційними технологіями, відіграватиме роль у встановленні зв'язків між кіберпростором, фізичним простором та людьми. Штучний інтелект (AI) може стати основою 6G, щоб він був рідним і повсюдно, щоб зробити кожен компонент 6G інтелектуальним. Також інтерактивність буде однією з головних складових 6G. Він збагатить повсякденне життя, забезпечуючи захоплюючий і тактильний досвід користувачам. На відміну від попередніх поколінь мобільних наземних систем, орієнтованих на підключення, 6G слід розглядати як суміш зв'язку, а також кіберпростору, фізичного простору, інтелекту та інтерактивності.

Перед детальним обговоренням сценаріїв використання 6G та їх застосування (випадків використання), основних ключових показників ефективності в Розділі 3 та відповідних технологій у Розділі 4, короткі описи кіберпростору, інтерактивності, інтелекту та підключення надаються таким чином:

- Кіберпростір: усі речі, включаючи простір, час і навіть думки, можна оцифрувати.

- Інтерактивність: люди можуть отримати доступ до кіберпростору за допомогою високотехнологічних сенсорних пристроїв, які можуть дозволити їм відчувати себе так, ніби вони насправді присутні в місці, що цікавить, безпосередньо взаємодіючи з його віртуальним оточенням, а також з іншими користувачами.
- Інтелект: штучний інтелект буде вбудований скрізь, не тільки в мережу, включаючи ядро, а й до дизайну бездротового інтерфейсу.
- Зв'язок: зв'язок між кіберпростором і фізичним простором забезпечується каналами зв'язку.

Вибрані вісім KPI для 5G були такими; пікова швидкість передачі даних, швидкість передачі даних, що відчуває користувач, затримка, мобільність, щільність з'єднання, енергоефективність, ефективність використання спектру та пропускна здатність області. З іншого боку, наразі незрозуміло, скільки і яких параметрів буде обрано для KPI 6G.

Як і класифікації в 5G, варіанти використання 6G, які мають подібні вимоги, можна розділити на групи або конкретні сценарії використання. Нижче наведено рекомендовані сценарії використання для 6G:

- Ультрамобільний широкосмуговий доступ (uMBB): варіанти використання за цим сценарієм вимагають набагато більшої швидкості передачі даних, ніж та, яка потрібна в сценарії використання 5G eMBB.
- Надмасштабний зв'язок машинного типу (uMTC): варіанти використання за цим сценарієм вимагають набагато більшої кількості одночасних з'єднань на простір, ніж необхідна в сценарії використання масового зв'язку машинного типу (mMTC) 5G.
- Надвисокоточний зв'язок (uHPC): варіанти використання за цим сценарієм вимагають значно меншої затримки, вищої надійності, більш точної синхронності або більш точного позиціонування, ніж ті, які потрібні в сценарії використання наднадійного зв'язку з низькою затримкою (URLLC) 5G. Ці вимоги виконуються окремо або в поєднанні один з одним.
- Розширене 3-вимірне покриття (e3DC): варіанти використання за цим сценарієм вимагають інтеграції наземного наземного мобільного та неземного супутникового зв'язку, включаючи дрони, повітряні та висотні платформні станції (HAPS), щоб забезпечити підключення до кожного куточка. на землі.
- Змішані сценарії використання.

Висновки та перспективи. Основною метою 6G є досягнення «інтелекту та зв'язку всюди», щоб забезпечити справді захоплюючий досвід і повсюдний широкосмуговий доступ до Інтернету кожній людині на земній кулі шляхом подолання існуючого цифрового розриву. Попередні покоління мобільних систем були розроблені як платформи для забезпечення підключення. В епоху 5G визначення мобільної системи було змінено, щоб створити екосистему для промисловості та бізнесу, акцентуючи увагу на вертикальних доменах. Тим не менш, досі, незважаючи на успіх розгортання 5G, він ще не довів своїх унікальних стратегій порівняно з попереднім поколінням. Щоб забезпечити по-справжньому захоплюючий досвід для кожної людини на земній кулі, 6G потребує не лише ряду нових можливостей за межами підключення, але й

значних удосконалень самого підключення.

Список використаних джерел:

1. Perspectives on 6G wireless communications [Електроний ресурс] – Режим доступу: https://www.sciencedirect.com/science/article/pii/S240595952100182X
2. A perspective on 6G: Requirement, technology, enablers, challenges and future road map [Електроний ресурс] – Режим доступу: *https://www.sciencedirect.com/science/article/abs/pii/S1383762121001302*

Білоус Максим Леонідович
Студент 5 курсу,групи КСДМ-51
(095)-731-97-00
maximu4bel@gmail.com
Державний університет телекомунікацій, м. Київ
Навчально-науковий інститут інформаційних технологій

ЯК ТЕХНОЛОГІЯ БЛОКЧЕЙН МОЖЕ ПРИНЕСТИ КОРИСТЬ ІНТЕРНЕТУ РЕЧЕЙ (IOT)

Блокчейн - збудований за певними правилами безперервний послідовний ланцюжок блоків (зв'язковий список), що містять інформацію. Зв'язок між блоками забезпечується не тільки нумерацією, але й тим, що кожен блок містить власну хеш-суму і хеш-суму попереднього блоку. 2021 рік – це рік, коли блокчейни еволюціонують від блискучих проривів на периферії до Інтернету багатьох блокчейнів. Блокчейн біткойн електризував своїх затятих шанувальників, але не знайшов застосування. Початкові інновації стануть ядром безпеки децентралізованого Інтернету Blockchains або Web 3.0. Основа для Web 3.0 підготує шлях до вибухового зростання децентралізованих програм.

Постановка задачі. Основним завданням для гравців IoT є захист інформації у всій екосистемі Інтернету речей. Уразливості безпеки роблять пристрої Інтернету речей легкою мішенню для розподілених атак «відмова в обслуговуванні», зловмисників і злому даних. Інтеграція Інтернету речей і блокчейну відкриває двері для нових можливостей, які за своєю суттю зменшують неефективність, підвищують безпеку та покращують прозорість для всіх залучених сторін, водночас забезпечуючи захищені міжмашинні транзакції. Поєднання цих технологій дозволяє відстежувати фізичні активи з моменту видобутку сировини, наприклад, і на кожному етапі ланцюга поставок до моменту його отримання у кінцевого споживача.

Мета дослідження. У розгортанні Інтернету речей існує багато проблем, зокрема витрати, безпека, конфіденційність та обмін даними. Метою дослідження є посилення важливих складових IoT.

Результати дослідження. Слід відзначити переваги інтеграції блокчейну та Інтернету речей.

Посилена безпека. Технологія Blockchain включає в себе безпеку з можливістю перевірки та дозволу транзакцій, здійснених довіреною стороною, а також шифрування під час передачі та зберігання даних. Технологія блокчейн забезпечує прозорість щодо того, хто має доступ, хто здійснює транзакції та

запис усіх взаємодій. Крім того, блокчейн додає рівень безпеки з точки зору шифрування, видалення єдиної точки збою та можливості швидкого визначення слабкої ланки у всій мережі.

Знижені витрати. Автоматизуючи етапи перевірки та обробки транзакцій на блокчейні, усю екосистему можна зробити проактивною за зниженою ціною.

Швидкість транзакцій. Особливо це стосується операцій з ланцюга поставок з кількома постачальниками, виробниками, дистриб'юторами та споживачами. Завдяки тому, що блокчейн певною мірою виконує роль спільної книги, недовірені сторони можуть обмінюватися даними безпосередньо одна з одною, усуваючи ручні процеси та збільшуючи швидкість транзакцій.

Проблема для кожної технології полягає в тому, щоб чітко визначити проблему або потребу клієнта, яку задовольняють.

Висновки та перспективи. Блокчейн і Інтернет речей можуть бути неймовірною комбінацією. Однак важливо зазначити, що блокчейн і Інтернет речей розвиваються не однаковими темпами.

Наприклад, блокчейн має такі обмеження, як масштабованість для роботи з великими обсягами даних, питання регулювання та конфіденційності даних, а також стандартизація, що є передумовами для прийняття підприємства. Технологія IoT також повинна довести, що інфраструктура безпечна, ефективна та стійка. Він все ще повинен подолати ці обмеження, перш ніж нові бізнес-рішення стануть основними елементами корпоративних технологій.

Список використаних джерел:

1. How Blockchain Technology Can Benefit the Internet of Things [Електронни ресурс] – Режим доступу: https://www.iotworldtoday.com/2021/05/31/how-blockchain-technology-can-benefit-the-internet-of-things/

2. What is blockchain [Електронни ресурс] – Режим доступу: https://www.oracle.com/cis/blockchain/what-is-blockchain/

Пінчук Дар'я Валеріївна
Студентка 5 курсу, групи КСДМ-51
Державного університету телекомунікацій
(098) 869 02 88
znodasha@gmail.com
Науковий керівник: Ткаченко Ольга Миколаївна,
кандидат технічних наук,
доцент кафедри Комп'ютерної інженерії
Державного університету телекомунікацій, м. Київ

ВИРІШЕННЯ ЗАГРОЗИ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ ЧЕРЕЗ КОНЦЕПЦІЮ КОМПАНІЇ CISCO "МЕРЕЖА БЕЗ КОРДОНІВ"

Мережева безпека сьогодні стала невід'ємною частиною комп'ютерних мережевих технологій. До мережевої безпеки відносять протоколи, технології, пристрої, інструменти і методи, що необхідні для забезпечення безпеки даних і зменшення загроз. Одним з найважливіших факторів розвитку мережевої безпеки можна віднести бажання

випередити зловмисних хакерів на один крок вперед. Фахівці з мережевої безпеки намагаються запобігти потенційним атакам, мінімізуючи наслідки атак в режимі реального часу. Ще одним фактором розвитку мережевої безпеки є забезпечення безперервності бізнесу. Вирішити всі ці питання можна застосувавши одну з таких технологій на базі концепції компанії Cisco "Мережа без кордонів".

Хмарна технологія відіграє все більшу роль у корпоративних мережах. Хмарні обчислення дозволяють організаціям використовувати такі послуги, як сховище даних або хмарні програми, щоб розширювати свої можливості та ємність без додавання інфраструктури. Хмара розташована поза традиційним периметром мережі, дозволяючи організаціям розміщувати ЦОД як усередині, і зовні традиційного міжмережевого екрана.

Поняття «хмарні обчислення» та «віртуалізація» найчастіше використовуються як взаємозамінні, насправді вони означають різні речі. Віртуалізація – основа хмарних обчислень, без неї хмарні обчислення та його широке використання були б неможливі. Хмарні обчислення відокремлюють програму від апаратних засобів. Віртуалізація відокремлює операційну систему від апаратного забезпечення.

Фактично хмарна мережа складається з фізичних та віртуальних серверів, які зазвичай розміщуються у центрах обробки даних. Проте центри обробки даних дедалі більше використовують віртуальні машини надання серверних послуг своїм клієнтам. Віртуалізація серверів дозволяє використовувати незадіяні ресурси та об'єднує кілька необхідних серверів. Таким чином, також забезпечується можливість існування різних операційних систем на одній апаратній платформі. Проте, віртуальні машини, також схильні до спеціальних цілеспрямованих атак.

Фахівцям з інформаційної безпеки потрібна проста, але при цьому комплексна стратегія, яка допоможе задовольнити потреби бізнесу та захистити ЦОД. Компанія Cisco розробила рішення щодо захисту ЦОД, яке дозволяє ефективно діяти в умовах непередбачуваного ландшафту загроз. Рішення Cisco захисту ЦОД блокує внутрішні та зовнішні загрози на периметрі ЦОД.

У минулому співробітники та інформаційні ресурси знаходилися в межах заздалегідь визначеного периметра, захищеного за технологією міжмережевого екрану. Співробітники зазвичай працювали на комп'ютерах компанії, підключених до корпоративної локальної мережі, які постійно контролювалися та оновлювалися відповідно до вимог безпеки.

Для впровадження тенденції BYOD компанія Cisco розробила концепцію "Мережа без кордонів". У Мережі без кордонів доступ до ресурсів може ініціюватися користувачами з різних позицій, з різних типів кінцевих пристроїв з використанням різних способів підключення. Використання такої концепції стало можливим завдяки використанню у цій технології хмарної технології.

Для реалізації такого «розмитого» периметра мережі Cisco підтримують функції управління мобільними пристроями (Mobile Device Management, MDM). За допомогою функцій MDM забезпечується безпека, моніторинг та управління мобільними пристроями як корпоративними, так і особистими. До

пристроїв з підтримкою та під керуванням MDM відносяться не лише «кишенькові» пристрої, такі як смартфони або планшети, але й ноутбуки та настільні обчислювальні пристрої.

Список використаних джерел

1. https://www.cisco.com/c/dam/global/ru_ua/training-events/downloads/borderless_security_voilibma.pdf .
2. https://www.cisco.com/c/uk_ua/products/security/cloudlock/index.html .

Капінус Артем Романович
студент 5 курсу, групи КСДМ-51
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
Kapinusartem.main@gmail.com
Науковий керівник: Ткаченко Ольга Миколаївна,
доктор технічних наук, професор,
завідуюча кафедрою Комп'ютерної інженерії
Державного університету телекомунікацій м. Київ

МЕТОДИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ЯКІ ПОШИРЮЮТЬСЯ ПРИ ПРОГРАМУВАННІ РОБОТІВ

Штучний інтелект (ШІ) і робототехніка – це потужна комбінація для автоматизації завдань всередині та поза заводом. Останніми роками AI стає все більш поширеним у роботизованих рішеннях, впроваджуючи гнучкість та можливості навчання в раніше жорстких програмах. Хоча штучний інтелект все ще знаходиться на стадії зародження, він став технологією, яка перетворює деякі додатки у виробничому секторі, хоча багато таких, які ще не відчули впливу.

Постановка проблеми. Відбір інформації та визначення основних проблем. Розглянути та проаналізувати проблеми використання штучного інтелекту при створенні роботів

Мета дослідження. Дослідження сучасної логіки програмування роботів. Аналогії з репрезентацією в минулому. Розуміння однакових принципів людини і машини.

Результати дослідження. Штучний інтелект – це галузь інформатики, яка розробляє інтелектуальні комп'ютерні системи, тобто системи, які мають можливості, які ми традиційно асоціюємо з людським розумом – розуміння мови, навчання, здатність міркувати, розв'язувати проблеми тощо. Основними особливостями ШІ є розуміння мови, навчання та здатність мислити та діяти. Робота зі штучним інтелектом можна схематично представити як основу, в якій розташовані Знання, і чотири стовпи, якими є розуміння, сприйняття, комунікація та навчання. Основою інтелекту роботів, як і природного інтелекту, є знання. Інтелект робота ґрунтується насамперед на наявності в нього моделі пам'яті самого себе та свого робочого середовища. Ця модель є

знанням робота. Знання – це модель роботи в операційному середовищі, представлена у вигляді безлічі взаємопов’язаних структур, які називаються поняттями, твердженнями, навичками, явищами. Поведінка – це здатність робота формувати послідовність своїх дій з урахуванням впливу внутрішніх і зовнішніх факторів для досягнення мети. Наявність інтелекту в роботі та його рівень багато в чому визначають поведінку робота. Поведінка зазвичай оцінюється за кількома параметрами. З точки зору робототехніки, найважливіше – оцінити ступінь усвідомленості поведінки робота. Поведінку робота можна назвати осмисленою, коли для досягнення поставленої мети робот оцінює ситуацію, свої дії та їх наслідки, виконує процедури та алгоритми Мислення, яке виконує Мислення, Прогнозування та Планування. Робот використовує: - факти, отримані в процесі сприйняття свого стану та стану операційного середовища; - факти, припущення та можливі події, витягнуті з його пам'яті; - правила логічного висновку, прогнозування та планування. Крім того, на поведінку роботів може впливати спілкування з людьми чи інші види роботи та навчання, яке можна поєднувати зі спілкуванням. Таким чином, осмислена поведінка ініціює роботу всіх компонентів інтелекту робота. З іншого боку, рефлекторна поведінка використовує мінімум інтелектуальних ресурсів. Алгоритми рефлекторної поведінки використовують спеціальні правила, такі як: P: якщо A і S, то D

Тут: P — назва правила; A - вихідні посилки, логічний вираз, складений з Фактів і Припущень, надійність яких визначає можливість використання Навику; S - цільові налаштування, логічний вираз, складений з Припущень, надійність яких є метою використання Навику; D - дія-робота, визначена одним з навичок. Правила такого типу не дозволяють роботі думати, передбачати, планувати свої дії, оскільки наслідків застосування дії, визначеної Правилом, він не знає. Їх немає в структурі. Якщо робот використовує тільки Правила цього типу, то відпадає потреба в алгоритмах Осмислення, і поведінка робота стає рефлексивним. Однак, навіть з Reflex Behavior, робота з ініціювання Правил вимагає початкових посилок, фактів і припущень про вас і стан робочого середовища. Для отримання цієї інформації використовуються алгоритми сприйняття та комунікації. Вони також можуть бути надзвичайно простими або взагалі відсутніми, якщо модель світу, що зберігається в пам'яті робота, представлена у вигляді набору необроблених сигналів від датчиків. У цьому випадку поведінка робота стає сенсорно-рефлекторною, і вона однозначно визначається лише сигналами, що надходять від датчиків, які безпосередньо ініціюють дії робота. Рефлекторна поведінка має певні переваги перед осмисленою. Для його реалізації немає необхідності розробляти складні правила розуміння та програми їх обробки. Найпоширенішим способом реалізації рефлекторної поведінки є створення Правил у вигляді таблиць, рядки яких містять комбінацію Фактів і Припущень, що становлять вихідні передумови, цільові налаштування та алгоритми дій, які має виконувати робот.

Висновки та перспективи. Використання штучного інтелекту робить можливим або спрощує багато завдань, однією з яких є програмування роботів. Хоча людство все ще знаходиться на самому початку реалізації ідеальної машини, принципи та бачення не змінилися з початку ери робототехніки. Ви

бачите, як концепції 50-річної давності стають все більш реальними, виконуючи функції, закладені в них через багато поколінь.

Список використаних джерел:

1. *О. П. Александров // Роботы и искусственный интеллект*
2. *Зюзин, Б. Ф // Теория дистортности в оценке IQфактора объектов искусственного интеллекта*

Ярмола Микола Володимирович,
студент 5 курсу, групи КСДМ-51
(099) 264 28 13
nick.yarmola.99@gmail.com
Науковий керівник: **Ткаченко Ольга Миколаївна,**
доктор технічних наук, професор,
завідуюча кафедрою Комп'ютерної інженерії
Державного університету телекомунікацій, м. Київ

ЗАСТОСУВАННЯ ОБЧИСЛЮВАЛЬНИХ ПОТУЖНОСТЕЙ AMAZON WEB SERVICES EC2 ДЛЯ ПОБУДОВИ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ

Постановка задачі. В умовах стрімкого розвитку хмарних технологій все більше компаній стають зацікавленими в тому, щоб емігрувати власну серверну інфраструктуру в датацентри сторонніх провайдерів. Одним з таких постачальників послуг є Amazon Web Services, зокрема їхній сервіс Elastic Compute Cloud.

Мета дослідження. Визначення основних переваг використання серверних потужностей стороннього провайдера замість обслуговування власної інфраструктури.

Результати дослідження. Amazon Web Services - це найбільший у світі постачальник платформи хмарних в обчислень в оренду, який пропонує різноманітні інструменти під певні потреби, зокрема Amazon Elastic Compute Cloud (EC2) і Amazon Simple Storage Service (S3).

Amazon EC2 є найбільш поширеним сервісом, який підтримує різні типи віртуальних серверів: оптимізовані для використання як хмарне сховище, оптимізовані для великих обчислень, універсальні. Ці сервери можна фізично розмістити в різних регіонах світу (Європа, США, Азія) для досягнення високого рівня доступності.

Для кінцевого споживача однією з найважливіших характеристик хмарних серверів є можливість масштабування, тобто збільшення об'єму пам'яті, ядер процесора, кількості виходів в мережу тощо. Це важливо при зростанні кількості навантаження на сервіси, які розміщені у хмарі. При використанні традиційних, "фізичних" серверів, ця процедура забрала б чимало коштів та часу. Крім цього, керування серверами у хмарі може відбуватись через веб-інтерфейс з будь-якої точки світу та підтримує виконання будь-яких

конфігурацій, що спрощує роботу системним адміністраторам компаній.

Висновки та перспективи. Безумовно, є компанії, якім критично необхідно всі обчислення проводити на власних серверних потужностях, а не тих, що пропонуються хмарними провайдерами. Проте для більшості компаній, які зацікавленні в оптимізації витрат на серверне обладнання та його адміністрування, Amazon Web Services є тим рішенням, яке дозволить оптимізувати і витрати коштів, і витрати часу, і також підвищити відмовостійкість та доступність сервісів.

Список використаних джерел

1. Wikipedia [Електронний ресурс] - режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Amazon_Web_Services
2. Amazon EC2 features [Електронний ресурс] - режим доступу до ресурсу: https://aws.amazon.com/ec2/features/?nc1=h_ls

Тонкий Ілля Олегович
Студент 5 курсу, крупи КСДМ-51
(066)4418967
otitoilegit@gmail.com
Науковий керівник: Ткаченко Ольга Миколаївна,
доктор технічних наук, професор,
завідуюча кафедрою Комп'ютерної інженерії
Державного університету телекомунікацій м. Київ

НОВІТНІ СИСТЕМИ БПЛА

На сьогоднішній день сфера IT заполонила майже весь простір життя людей, проте досі дуже мала кількість людей вміє програмувати та розробляти ті самі технології, які ми використовуємо кожен день. Насамперед хочу розповісти про актуальну тему для нашої країни у цей час – БПЛА.

Постановка задачі. Дана публікація має на меті продемонструвати актуальні безпілотники, а також дослідити їх принципи роботи та порівняти відмінності підходів до вирішення різних задач.

Мета дослідження. Аналіз напрямків у тестуванні продуктивності БПЛА.

Що таке БПЛА? Безпілотник, є літаком без екіпажу. Ним керують на відстані, або він використовує наперед запрограмовану автоматичну систему навігації.

Для чого їх використовують? Безпілотники бувають різних форм і розмірів, використовують як у військових, так і в цивільних цілях, наприклад, для наукових досліджень, для промислових спостережень. Також їх використовують правоохоронці. Проте основне призначення безпілотників все ж військове – розвідка та бойові операції.

Історично склалося так, що безпілотники класифікують як — літакові та мультироторні. Мультироторні можна розділити за кількістю гвинтів:

монокоптери, квадрокоптери, гексакоптери тощо. Такі БПЛА набули широкого поширення, оскільки їм не потрібні додаткові пристрої для зльоту та посадки. Нещодавно з'явився третій клас БПЛА – конвертоплани. Але така конструкція найчастіше зустрічається у спеціалізованих розробках.

Конвертоплан – безпілотний літальний апарат, що представляє комбінацію літака та мультикоптера з можливістю моментального переходу між двома польотними режимами. Ключовою відмінністю моделі є новий тип управління – воно здійснюється за рахунок незалежно змінюваних векторів тяги двигунів. Також розробили систему автоматичного керування, яка підтримує перехід між режимами польоту. Система забезпечує стабільний політ як у режимах мультикоптера та літака, так і в режимі часткової конвертації.

Крім прототипу пристрою з поворотними механізмами, було розроблено і літак з вертикальним зльотом. Така конструкція дозволяє вирішувати поставлені завдання більш простим способом. Апарат можна використовувати для доставки невеликих вантажів у важкодоступні місця, причому навіть у зонах стихійних лих, так як пристрій здатний сісти практично на будь-яку поверхню.

Висновки та перспективи. Отже, БПЛА зараз набуває велику популярність серед громадських сфер життя, проте у наш час в нашій країні вони успішно допомагають у виконанні поставлених завдань.

Список використаних джерел:

1. https://habr.com/ru/company/leader-id/blog/491770/
2.https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D0%B2%D0%B5%D1%80%D1%82%D0%BE%D0%BF%D0%BB%D0%B0%D0%BDhttps://dic.academic.ru/dic.nsf/ruwiki/977304

Філімець Ростіслав Ігорович
Студент 5 курсу,групи КСДМ-51
(098)-105-66-61
rfilimec@gmail.com
Державний університет телекомунікацій м. Київ
Навчально-науковий інститут інформаційних технологій

ТЕХНОЛОГІЯ ІДЕНТИФІКАЦІЙНОГО МОДУЛЯ АБОНЕНТА ISIM

SIM картка – постійний супутник будь-якого мобільного телефону. Але останнім часом почали з'являтися нові типи SIM карт, наприклад, Nano-SIM, e-SIM. Ринок IT стрімко розвивається. Днями компанія Qualcomm, один із найбільших постачальників чіпів зв'язку на ринок електроніки, спільно з оператором Vodafone та промисловою групою Thales продемонструвала в роботі новий стандарт SIM, який отримав назву iSIM. За словами авторів проекту цей стандарт є новим етапом еволюції SIM. Попередня була технологія eSIM, яка давала можливість отримати доступ до послуг зв'язку операторів без встановлення картки SIM. Але для eSIM все ж таки був потрібний окремий модуль зв'язку, а ось iSIM вбудовується прямо в SoC. Раніше компанія розповідала про iSIM, але дуже коротко, тепер показано працюючий пристрій на базі цієї технології з розкриттям особливостей новинки.

Постановка задачі. З кожним роком нові елементи в корпусі смартфона займають все більше та більше місця. Така тенденція змушує виробників шукати нові рішення для того щоб зменшити розмір елементів в сучасному

смартфоні. Нове рішення від компанії Qualcomm має на меті вирити дану проблему не стандартним способом.

Метою дослідження. Метою дослідження є можливості технології iSIM та можливе використання даної технології в сучасності та майбутньому.

Результати дослідження. Поки що iSIM ще доопрацьовується, але прототип мобільного процесора із вбудованим модулем зв'язку вже виготовлено та продемонстровано. Йдеться не про якісь екзотичні чіпи, а про флагман 2021 року від Qualcomm — процесор Snapdragon 888 5G. Є й сучасніший чіп виробництва тієї ж компанії, який отримав назву Snapdragon 8 Gen 1, але тестувати iSIM автори проекту вирішили саме з 888 процесором.

Партнерами Qualcomm у цьому проекті є оператор мобільного зв'язку Vodafone та компанія Thales, яка є виробником інформаційних систем для авіакосмічної галузі, морської галузі та військових.

У ході демонстрації автори проекту використовували смартфон зі складним екраном Galaxy Z Flip3 5G, мабуть, для видовищності.

Оскільки технологія допрацьовується, автори проекту не розповіли про дату появи iSIM у загальному користуванні. Лише побіжно згадали про те, що, можливо, вихід технології на ринок відбудеться вже в 2023 році. Крім того, нічого не було сказано про те, які пристрої можуть отримати цю технологію. Смартфони, планшети або ноутбуки - можливо, з допрацьованими чіпами будуть сумісні всі типи пристроїв, але цілком можливо, що першою категорією девайсів з iSIM стануть саме смартфони.

iSIM має декілька позитивних моментів. Відсутність необхідності додавати окремий модуль зв'язку та «обв'язування», включаючи лоток для SIM-карток. Його немає у тих телефонів, що підтримують виключно eSIM, але в цьому випадку окремий модуль зв'язку та «обв'язування» до нього все ж таки присутні. А ось у технології, що розвивається iSIM, нічого цього немає. Відповідно, звільнене місце, якого на платі завжди не вистачає, можна використовувати для розміщення додаткових компонентів камери, інших модулів або акумулятора збільшеної ємності.

Сумісність із eSIM. Іншими словами, операторам зв'язку не потрібно змінювати процедуру реєстрації мобільних номерів. Можна використовувати той самий QR-код для прив'язки номера до певного пристрою. Це просто і здебільшого працює без проблем. Оскільки операторам мобільного зв'язку майже нічого не доведеться змінювати, вони швидше за все підуть назустріч ініціативі і почнуть адаптувати технологію. Приклад того ж Vodafone, ймовірно, послужить додатковим стимулом для компаній зв'язку з різних країн. Та ж Motorola Razr 2019, в якій використовується лише модуль eSIM, може бути перевипущена з новим процесором.

Можливість додавання модулів зв'язку не лише в мобільні телефони, а й у ноутбуки або планшети. У деякі моделі окремий модуль SIM і так вбудовується, але це ускладнює конструкцію девайсу. Якщо модуль зв'язку буде вбудований в SoC, до мобільної мережі можна буде підключати пристрої будь-якої категорії, куди можна встановити процесори нового типу.

Висновки та перспективи. Отже, можна дійти до висновку, що технологія iSIM э дуже переспективною, та в майбутньому витіснить своїх

конкурентів. Складнощів із додаванням, наприклад, ноутбуків, бути не повинно. Справа в тому, що Microsoft додала розширену підтримку ARM-процесорів Qualcomm до нової версії своєї операційної системи. Більш того, сама компанія Qualcomm наприкінці 2021 представила чіп для портативних ПК на Windows. Це Snapdragon 8cx Gen 3, виконаний за 5-нм техпроцесом. Тоді процесори були чистими, тобто без модуля зв'язку iSIM. Але зараз нічого не заважає його додати. За словами представників проекту, технологія дозволяє розширити можливості широкого спектру пристроїв, від ноутбуків та мобільних телефонів до IoT-пристроїв та окулярів віртуальної реальності. Більш того, автомобілі тепер теж можна буде постачати з iSIM, що дозволить власникам завжди бути на зв'язку у разі потреби.

Список використаних джерел:

1. https://kigen.com/resources/blog/sim-esim-isim-whats-the-difference/
2. https://timesofindia.indiatimes.com/gadgets-news/explained-what-is-isim-technology-and-how-it-may-change-the-use-of-sim-cards/articleshow/89031978.cms

Баглай Владислав Олегович
студент 4 курсу, групи ПД-42
(068) 780 14 97
baglai.vladyslav@gmail.com
Науковий керівник: **Негоденко Олена Василівна**
к.т.н., доцент завідувач кафедри Інженерії програмного забезпечення
Державного університету телекомунікацій, м. Київ

АКТУАЛЬНІСТЬ ВЕБ-ДОДАТКУ ДЛЯ КЕРУВАННЯ ТОРГІВЛЕЮ ТА СКЛАДСЬКОГО ОБЛІКУ

Сучасна тенденція ринку показує, що неможливо вести бізнес без IT. На даний момент існує багато SaaS продуктів для контроля торгівлі, облік складу. Проблема в тому, що значна частина з цих додатків це декстопні програми. Так як технології розвиваються, ринок IT росте, пропонує всі нові додатки — при інших рівних користувачах буде вибирати веб просто тому, що це зручніше. Якщо говорити про рішення для корпоративних клієнтів, то тут браузерні додатки незамінними. Вони гнучкі, універсальні, не вимагають попередньої підготовки середи, дозволяють економити фінанси компанії, апаратні ресурси, час співробітників.Використання сервісів для керування торгівлею та складського обліку, позитивно впливає на бізнес. Так як пришвидшуються процеси торгівлі та дозволяє зберігати великі данні про продажі, закупівлю. Це надає використовувати данні для аналітики, наприклад з допомогою якої можна покращити процеси маркетингу.

Постанова дослідження. Довести актуальність веб-додатку для керування торгівлею та складського обліку.
Мета дослідження. Метою дослідження є аналіз відсотків роздрібної та

оптової торгівлі на українському ринку.

Результати дослідження. За офіційними даними за 2021 рік кількість фопів зросла на 83257 або на 4%. З 2 млн. фопів роздрібна торгівля та оптова торгівля (без автотранспорта) має 38% (рис. 1) на початок 2022р..

Рисунок 1 Види діяльності за кількістю фопів на початок 2022 р.

Але це тільки зареєстровані данні. Також фактором того, що ринок розвивається є популярні маркетплейси. Rozetka в 2016 році стала маркетплейсом. А в 2018 році товарообіг на маркетплейсі Prom.ua виріс на 66,5% (рис. 2).

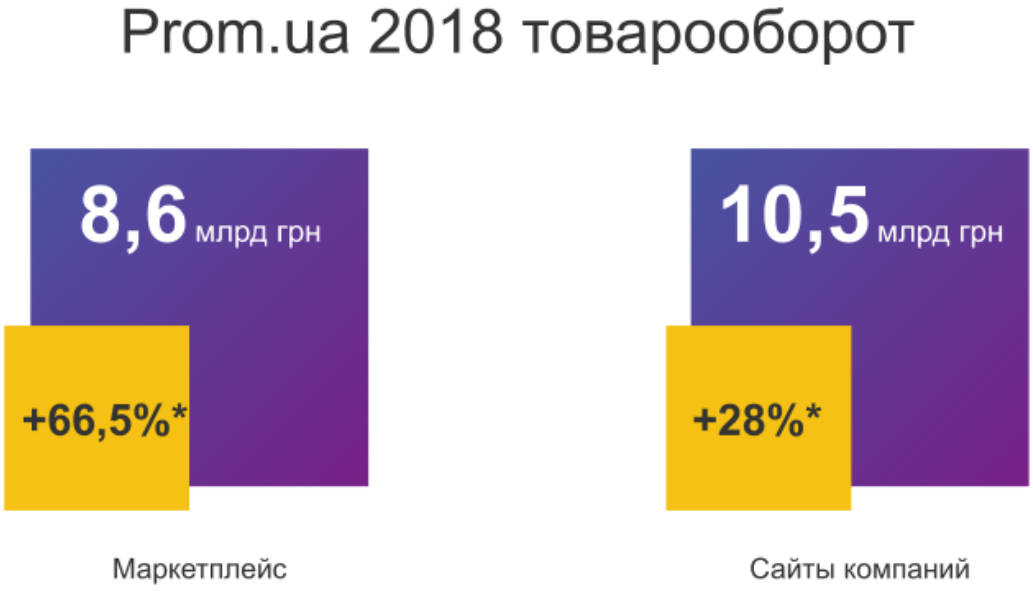

Рисунок 2 Товарообіг на найбільшому маркетплейсу Prom.ua

Висновки та перспективи. Оскільки кількість малого та середнього бізнеса лише зростає то і зростає потреба в додатках для бізнесу. Автоматизація

ведення складського обліку та керування торгівлею допоможе уникнути зайвих проблем при торгівлі. Значно підвищить швидкість торгівлі та допоможе опрацьовувати дані для маркетингу, це підвищить ефективність торгівлі. Також з факторів невелика кількість аналогів. Саму тому, веб-додаток для керування торгівлею та складського обліку надзвичайно актуальне в цей час.

Список використаних джерел:

1. Opendatabot [Електронний ресурс] : [Веб-сайт] – Режим доступу: https://opendatabot.ua
2. Мінфін [Електронний ресурс] : [Веб-сайт] – Режим доступу https://minfin.com.ua
3. Приватний підприємець [Електронний ресурс] : [Веб-сайт] – Режим доступу http://chp.com.ua

Білоус Максим Леонідович
Студент 5 курсу групи КСДМ-51
(095)-731-97-00
maximu4bel@gmail.com
Державний університет телекомунікацій, м. Київ
Навчально-науковий інститут інформаційних технологій

ЗАСТОСУВАННЯ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ГАЛУЗІ МАШИНОГО НАВЧАННЯ

Кіберстрахування - це відносно новий тип перенесення корпоративної відповідальності. Подібний поліс потенційно дозволяє покрити збитки, пов'язані з порушеннями систем безпеки. Ринок такого страхування продовжує стрімко зростати, і сьогодні ми хочемо поговорити про те, хто є головним споживачем таких страховок, і що вони дають сервісним компаніям.

Постановка задачі. Компанії не готові брати на себе всі ризики, пов'язані з ІБ і вважають за краще ... купити страховку! За даними Standard & Poor глобальний ринок кіберстрахування на даний момент становить приблизно $ 5 мільйонів на рік. Однак його зростання прогнозується на рівні 20-30% щорічно протягом усього "недалекого майбутнього". Приблизно такої ж оцінки дотримуються в страховій компанії Munich Re, яка продає кіберполіси. Вони очікують збільшення ринку до $ 20 мільярдів вже до 2025.

Уряд США і інші авторитетні джерела неодноразово підкреслювали, що провайдери (MSPs) є основною метою для кіберзлочинців. Адже популярність різних хмарних сервісів робить їх справді дуже привабливою здобиччю. У разі успішного злому MSP всі замовники разом з їх даними, мережами і системами також виявляються скомпрометовані. Тому не дивно, що кіберстрахуванням хочуть в першу чергу скористатися саме провайдери, щоб зняти з себе тягар фінансової відповідальності перед своїми клієнтами "якщо що".

Метою дослідження. Метою дослідження є ризики в інформаційній безпеці.

Результати дослідження. Чому провайдерам потрібна кіберстрахування в першу чергу?

Якщо навіть MSP не пропонує сервісів в області кіберзахисту, замовники все одно очікують, що їхні активи будуть захищені. І проведений після атак на Kaseya опитування 2021 Global MSP Benchmark Survey Report привів до

наступних висновків:

- MSP повідомили, що найбільшим викликом у 2021 році для їх клієнтів є забезпечення безпечної роботи співробітників з дому, IT - безпеку в цілому, а також підтримка безперервності бізнесу і можливостей аварійного відновлення.
- У числі найбільш популярних керованих сервісів з області безпеки: антивіруси, anti-malware, управління кінцевими точками, резервне копіювання серверів, установка патчів на ОС, а також безпеку електронної пошти.
- 63% відзначили, що протягом 2020 року всі їх замовники консультувалися з ними в питаннях вибору стратегії кіберзахисту і застосування кращих практик. І 37% відзначили, що кіберзахист є важливою точкою зростання для їх бізнесу.

Отже, MSP активно виходять на стежку кібербезпеки, і починають брати на себе частину відповідальності. Але це все одно неминуче - замовники все одно хотіли б перекласти на провайдера всі ризики, пов'язані з кібербезпекою, навіть якщо MSP не є безпосереднім учасником процесу. Звернемося за прикладом в заокеанські країни: Ohio manufacturing company подала в суд на свого MSP після того, як фірма втратила $ 1,7 мільйона в результаті продуманої фішинговою атаки, хоча провайдер не надавав їм сервіс кіберзахисту. А SolarWinds продовжує зазнавати труднощів через торішнього злому своїх керованих сервісів і підтримують їх систем. Експлойт, виявлений роком раніше, був опублікований ще в грудні 2020 року. Він дозволив зловмисникам проникати в мережі клієнтів компанії, в числі яких були навіть урядові структури США.

Ще один показовий приклад уразливості на стороні MSP - це атака Ransomware через рішення Kaseya. 2 липня 2021 року угруповання REvil використовувала уразливості в on-premise версії серверів Kaseya з популярними інструментами для віддаленого моніторингу та управління. В результаті були скомпрометовані близько 50 MSP і тисячі їх клієнтів. Атакуючі вимагали викуп в $ 25 000- $ 150. 000 с кожного з них, $ 5 мільйонів з провайдерів і $ 70 у Kaseya. Так що, якщо б все заплатили, вийшла б кругленька сума.

Висновки та перспективи. В результаті, незважаючи на зростання вартості кіберстрахування, сьогодні 60% MSP звертаються до страхових компаній і включають витрати на поліс до складу своєї стратегії зниження ризиків. І очікується, що ця частка тільки продовжить рости, в тому числі з-за дій регуляторів. Наприклад, в лютому 2020 року в Штаті Каліфорнія був прийнятий закон, який наказував би мати кіберстрахування всіх IT-контракторов уряду. Крім цього MSP, які оплачують кіберстраховку, допомагають своїм клієнтам пройти аудит, і тому наявність поліса кіберстрахування може стати конкурентною перевагою.

Список використаних джерел:

1. Інтернет-джерело:https://news.microsoft.com/ru-ru/microsoft-nvidia-megatron-turing-natural-language-generation/
2. Інтернет-джерело: https://habr.com/ru/news/

Рудий Андрій Сергійович,
студент 4 курсу, групи ПД-44
Державного університету телекомунікацій
(096) 805 42 28
andrey.rudy1@gmail.com
Науковий керівник: Дібрівний Олесь Андрійович,
Доцент кафедри Інженерії програмного забезпечення, доктор філософії
Навчально-науковий інститут Інформаційних технологій ***м. Київ***

ОСОБЛИВОСТІ РОЗРОБКИ ІГОР НА UNITY

Unity - міжплатформне середовище розробки комп'ютерних ігор, розроблене американською компанією Unity Technologies. Unity дозволяє створювати програми, що працюють на більш ніж 25 різних платформах, що включають персональні комп'ютери, ігрові консолі, мобільні пристрої, інтернет-програми та інші

По даним з аналізу Ларса Дусе, засновника gamedatacrunch.com, Unity займає більше 50% ринку. Чому ж так усім подобається Unity?

Як правило, ігровий двигун надає безліч функціональних можливостей, що дозволяють їх задіяти в різних іграх, в які входять моделювання фізичних середовищ, карти нормалей, динамічні тіні та багато іншого. На відміну від багатьох ігрових движків, Unity має дві основні переваги: наявність візуального середовища розробки і міжплатформенну підтримку. Перший фактор включає не тільки інструментарій візуального моделювання, а й інтегроване середовище, ланцюжок складання, що спрямоване на підвищення продуктивності розробників, зокрема етапів створення прототипів та тестування. Під міжплатформною підтримкою надається не тільки місця розгортання (установка на персональному комп'ютері, на мобільному пристрої, консолі тощо), але й наявність інструментарію розробки (інтегроване середовище може використовуватись під Windows та Mac OS).

Третьою перевагою називається модульна система компонентів Unity, за допомогою якої відбувається конструювання ігрових об'єктів, коли останні є комбінованими пакетами функціональних елементів. На відміну від механізмів успадкування, об'єкти в Unity створюються за допомогою об'єднання функціональних блоків, а не поміщення у вузли дерева успадкування. Такий підхід полегшує створення прототипів, що є актуальним при розробці игр.

Що до недоліків - це обмеження візуального редактора під час роботи з багатокомпонентними схемами, як у складних сценах візуальна робота ускладнюється.

Другим недоліком називається відсутність підтримки Unity посилань на зовнішні бібліотеки, роботу з якими програмістам доводиться налаштовувати самостійно, і це ускладнює командну роботу.

Ще один недолік пов'язаний із використанням шаблонів екземплярів (англ. prefabs). З одного боку, ця концепція Unity пропонує гнучкий підхід візуального редагування об'єктів, але з іншого боку, редагування таких шаблонів є складним. Також, WebGL-версія двигуна, в силу специфіки своєї архітектури (трансляція коду з C # C++ і далі в JavaScript), має ряд невирішених

проблем з продуктивністю, споживанням пам'яті і працездатністю на мобільних пристроях.

Обміркувавши все, мною було прийнято рішення розробити власну гру у жанрі Платформер за допомогою двигуна Unity та його можливостей. Завдяки простоті роботи з Unity я швидко освоївся у цьому інструменті для початку розробки власної гри. Завдяки гнучкості та універсальності, я планую реалізувати гру із власними унікальними фічами.

Список використаних джерел:

1. Unity [Електронний ресурс]. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Unity_(рушій_гри)
2. Unity [Електронний ресурс]. – Режим доступу до ресурсу: https://unity.com/
3. Розробка платформеру на Unity [Електронний ресурс]. – Режим доступу до ресурсу: https://habr.com/ru/company/microsoft/blog/236125/

Савенко Вадим Володимирович
студент 4 курсу, групи ПД-44
Державного університету телекомунікацій
(066) 540 45 30
savenko.vadym@gmail.com
Науковий керівник Дібрівний Олесь Андрійович
доктор філософії, доцент кафедри Інженерії програмного забезпечення
Державного університету телекомунікацій, м. Київ

СУЧАСНІ ПРИНЦИПИ РОЗРОБКИ КАЗУАЛЬНИХ ІГОР

Ігрова індустрія завжди була передовою нішею у розвитку і запровадженні новітніх технологій. Явище масовості казуальних ігор нерозривне з сучасним прогресом. Наступна теза звертає увагу на нові тенденції та принципи розробки успішного ігрового продукту..

Казуальна гра є цікавою у своїй розробці. Адже, якщо говорити про цей тип ігор, то кожен дизайнер-розробник має справу з створенням проектів продуманих на алгоритмічному та патерновому рівнях.

Самі по собі казуальні ігри прийнято вважати простими. І основна їх ідея бути цікавими пересічній більшості людей. У процесі дизайну майбутньої гри варто враховувати базові складові без яких такі ігри втратили б свою ідентичність. Є такі очікувані від гри характеристики:

- Веселий та простий ігровий процес, що базується на вже зрозумілому і знайомому для людей
- Простота у взаємодії, яка представлена незначною кількістю варіантів для дій
- Короткість ігрового періоду, що дає змогу грати в будь-яку вільну хвилину

- Вже знайомі ігрові елементи з реальних ігор

Реалізовуючи в моделюванні гри ці особливості на етапі проектування розробник може бути впевненим у якості створюваного ним проекту та у обов'язковій успішності після релізу.

Опісля закінчення концепту гри і розуміння моделі ігрового процесу програміст зазвичай удосконалює ігрові механіки. Адже саме вони і стають базовою приваблюючою силою, якої потребує успішний і привертаючий увагу широких мас проект. Таким чином навіть розроблена студентом гра приречена на впізнаваність.

Механік було створену велику кількість і основна омана у казуальних іграх – це те, що вони прості як у ігровому процесі так і в ігрових сценаріях. Хоча на практиці примітивні пророблені програмістом алгоритми можуть давати високу складність комбінацій гравцем принципів гри. Та для того хто провів хоча б базовий аналіз сучасного ринку подібних аналогів, стає ясним те, що сучасний ринок потребує акценту на графічність і вражаючу, а головне приваблюючу візуальність, тоді як динаміка гри може бути забезпечена гарно спроєктованими ігровими скриптами.

Наступний за раціональним ходом життєвого циклу розробки і в призмі створення казуальної гри є етам художньої реалізації концепту. У розробці ігор звичною справою є елементи мистецтва, тому гарний розробник звісно вміє знайти необхідні навички для зображення ігрових елементів. І звісно пам'ятаємо про важливість акценту на яскравості та динамічності візуального складу гри.

У заключній частині важливо звісно обробити всі, заважаючі грі, моменти як ігрового досвіду, так і відповідних візуальних фрагментів. Так у результаті гарний розробник, пройшовши цикл створення програмного рішення, отримує повноцінний продукт, який чекає не лише на реліз, а і на успіх.

Список використаних джерел:

1. *Tracy Fullerton // Game Design Workshop: A Playcentric Approach to Creating Innovative Games, Fourth Edition*
2. *Wlad Marhulets // GAMEDEV: 10 Steps to Making Your First Game Successful*
3. *Joe Hocking // Unity in Action: Multiplatform game development in C#*