

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ
ХАРЧОВИХ ТЕХНОЛОГІЙ**



ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

**80 НАУКОВОЇ КОНФЕРЕНЦІЇ
ВИКЛАДАЧІВ АКАДЕМІЇ**

Одеса 2020

Наукове видання

Збірник тез доповідей 80 наукової конференції викладачів академії
7 – 8 травня 2020 р.

Матеріали, занесені до збірника, друкуються за авторськими оригіналами.
За достовірність інформації відповідає автор публікації.

Рекомендовано до друку та розповсюдження в мережі Internet Вченою радою
Одеської національної академії харчових технологій,
протокол № 15 від 05.05.2020 р.

Під загальною редакцією Заслуженого діяча науки і техніки України,
Лауреата Державної премії України в галузі науки і техніки,
д-ра техн. наук, професора Б.В. Єгорова

Укладач Т.Л. Дьяченко

Редакційна колегія

Голова Єгоров Б.В., д.т.н., професор
Заступник голови Поварова Н.М., к.т.н., доцент

Члени колегії: Амбарцумянц Р.В., д-р техн. наук, професор
Безусов А.Т., д-р техн. наук, професор
Бурдо О.Г., д.т.н., професор
Віннікова Л.Г., д-р техн. наук, професор
Гапонюк О.І., д.т.н., професор
Жигунов Д.О., д.т.н., доцент
Іоргачова К.Г., д.т.н., професор
Капрельянц Л.В., д.т.н., професор
Коваленко О.О., д.т.н., ст.н.с.
Косой Б.В., д.т.н., професор
Крусір Г.В., д-р техн. наук, професор
Мардар М.Р., д.т.н., професор
Мілованов В.І., д-р техн. наук, професор
Павлов О.І., д.е.н., професор
Плотніков В.М., д-р техн. наук, доцент
Станкевич Г.М., д.т.н., професор,
Савенко І.І., д.е.н., професор,
Тележенко Л.М., д-р техн. наук, професор
Ткаченко Н.А., д.т.н., професор,
Ткаченко О.Б., д.т.н., професор
Хобін В.А., д.т.н., професор,
Хмельнюк М.Г., д.т.н., професор
Черно Н.К., д.т.н., професор

Основа її спиралася на хещированіє, задачу візантійських генералів, доказ Меркла. Головні переваги блокчейна це відсутність третьої сторони, забезпечення рівноправності бравших участь суб'єктів, децентралізація, всебічний нагляд, множинна перевірка даних, здатність підтримувати достовірність даних, неможливість редагування історії, доступність інформації.

Провідні платформи блокчейна, що пропонують використовувати смартконтракти для різноманітних цілей це Ethereum та Hyperledger. Smart contracts Ethereum – це коди на мовах Solidity або Vyper. Це пріоритетні мови Ethereum. Ланцюгової код Hyperledger Fabric може бути розроблений на різних мовах. Обидві платформи з відкритим початковим кодом.

Технологія розподіленого реєстру використовується в створенні стандартів постквантових криптографічних примітивів. В даний час це стандарти Держспецзв'язку ДСТУ 7564: 2014, ДСТУ 7624: 2014, ДСТУ 8845: 2019.

Зараз в світі йде впровадження блокчейна в сферу освіти, доступу до наукових матеріалів, обміну науковими знаннями та безліч інших сфер. Блокчейн може підняти систему управління на інший рівень відкритості та прозорості. Блокчейн має потенціал для створення робочих місць, економії коштів компанії і поліпшення економічного зростання.

Література

1. Олейников Р. Матеріали конференції. Харківський національний університет ім. Каразіна.
2. Черников М. Матеріали доповіді. Блокчейн 2019.
3. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World / Don Tapscott // Alex Tapscott. – 2016. – 324 с.
4. Blockchain: Blueprint for a New Economy / Melanie Swan. – 2015. – 152 с.
5. «Bitcoin in Brief» / Ben Isgur. – 2014. – 23 с.
6. Bitcoin Transaction Malleability and MtGox / Christian Decker// Roger Wattenhofer – 2016. – 14 с.
7. The Bitcoin Backbone Protocol: Analysis and Applications / Juan A. Garay. 2017. – 44 с.

ПРИНЦИПИ ПОБУДОВИ ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЇ

Владімірова В.Б., ст. викладач

Одеська національна академія харчових технологій, м. Одеса

Швидкий розвиток інформаційного ринку, інформаційного продукту призвів до того, що жодна електронна система – будь то державна або комерційна, не може обходитися без захисту інформації.

Ще у минулому столітті з'явилася потреба розроблялися різні методи, концепції захисту інформації. Але дуже швидко виникло питання розробки єдиного підходу до цієї проблеми. Це привело до створення політик безпеки інформації, які об'єднують у собі звід законів, правил, обмежень, рекомендацій, інструкцій тощо, які визначають порядок оброблення, розповсюдження та захисту інформації [1], [3].

Побудова інформаційної політики безпеки включає створення моделі політики, в якій наводиться її формальний опис та яка повинна використовуватися як під час проектування системи, так і під час перевірки та верифікації захищеності системи. Модель повинна узгоджуватися з нормативними документами системи технічного захисту інформації, ДСТУ, існуючими законами, внутрішніми правилами, визначати механізми та алгоритми захисту, та відповідати наступним вимогам:

- доступність;
- цілісність;
- конфіденційність;

— підзвітність.

Всі ці вимоги формують захищеність системи. На їх основі розробляється комплекс засобів захисту, який оснований на взаємодії наступних підсистем:

— розподілення повноважень;

— аудиту (реєстрація, облік);

— ідентифікації та автентифікації

— контролю та забезпечення цілісності інформації;

— криптографічних функцій (шифрування, цифровий підпис, генерування ключів та інше);

— антивірусного захисту.

Перш за все проводиться оцінка ризиків системи завдяки якій визначається що, від чого і як треба захищати. В процесі аналізу ризиків, по-перше, необхідно класифікувати всі активи (апаратуру, користувачів та персонал, документацію, програмне забезпечення та інше), і, по-друге, ідентифікувати можливі загрози для цих активів (несанкціонований доступ, підробка та порушення цілісності, віруси та інше) [2].

Після цього переходять до реалізації задач політики безпеки інформації, використовуючи обрану модель політики. Створення формальних моделей складний процес, який вимагає інтерпретації для застосування в реальних системах. Але лише за допомогою моделей безпеки, які опираються на математичну теорію, можна довести безпеку системи. Важливо відзначити, що затрати на розробку захисту не повинні перевищувати вартості ресурсу, що захищається.

Основними видами математичних моделей безпеки є мандатна, дискреційна, рольова, ізолюваного програмного середовища та безпеки інформаційних потоків [3]. Як найвідоміші можна відмітити перші три.

Дискреційна система є однією з найбільш поширених у світі. Вона базується на тому, що всі суб'єкти та об'єкти системи повинні бути ідентифіковані та права доступу суб'єкту системи до об'єкту можуть визначатися на основі зовнішніх стосовно системи правил. Суб'єкт, який є власником об'єкту може на свій розсуд давати іншим суб'єктам права доступу та відбирати ці права теж. Реалізується цей тип моделі за допомогою так званої матриці доступу. Проста реалізації системи сприяє її розповсюдженню. Але низка суттєвих недоліків приводить до більш чіткої та досконалої мандатної моделі політики безпеки.

Мандатна модель включає в себе однозначну ідентифікацію всіх об'єктів та суб'єктів системи, визначення та співставлення міток суб'єкту та міток об'єкту. Мітка суб'єкта визначає рівень його повноважень. Мітка об'єкта – ступінь його конфіденційності, яка визначає цінність інформації що в ньому міститься. Основною метою цього типу моделі є запобігання витоку інформації від об'єктів з високим рівнем доступу до об'єктів з низьким рівнем доступу. На тлі всіх переваг цієї системи виділяються суттєві недоліки, такі як складна практична реалізація та потреба використання значних ресурсів системи.

Ролева політика безпеки є розвитком дискреційної політики. Вона більш гнучка та близька до реального життя, тому що права доступу суб'єктів формуються згідно з їх ролями (повноваженнями та обов'язками).

Останнім етапом побудови політики безпеки інформації є її підтримка, яка здійснюється шляхом проведення аудиту вторгнень у систему, виявлення вад системи захисту.

Література

1. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – Київ, – 1999. – 16 с.

2. Хохлачова Ю. Політика інформаційної безпеки об'єкта. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – Т. 2, – вип. 24. – С. 23-29.

3. Грайворонский М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. –

ВИКОРИСТАННЯ PWA ТЕХНОЛОГІЇ ПРИ РОЗРОБЦІ КРОСПЛАТФОРМЕННИХ ДОДАТКІВ

Тройніна А.С., к.т.н., доцент

Одеська національна академія харчових технологій, м. Одеса

Сучасне програмне забезпечення має запускатися на великій кількості різних платформ, у кожній з яких свої апаратні особливості і можливості. Для того щоб досягти максимальної зручності для користувача, багато компаній розробляють продукт безпосередньо під кожну платформу, тим самим збільшуючи фінансові та часові витрати на розробку і підтримку в кілька разів. Для розробки універсальної програми, яка працює на всіх пристроях, розробнику необхідно зробити 5 окремих додатків: для Windows, для MacOS, для Linux, для Android і IOS. Таким чином стає актуальним розробка програми, яка буде працювати не тільки на різних операційних системах, але ще й на ноутбуках з Chrome OS, Smart TV і інших пристроях, пов'язаних з інтернетом речей.

Проведено детальний аналіз наявних рішень і підходів, які можуть спростити і здешевити виробництво кросплатформених додатків. На основі даних досліджень було запропоновано застосувати технологію Progressive Web App (PWA) [1].

PWA – це новий підхід розробки Web додатків, запропонований Google. В основі нього лежать звичайні і всім відомі технології: HTML, CSS і Javascript. Але додаючи нові технології поверх цієї основи і слідуючи 10 основам концепту запропонованими Google можна зробити передовий прогресивний додаток. На рис. 1 представлено опис технології PWA.

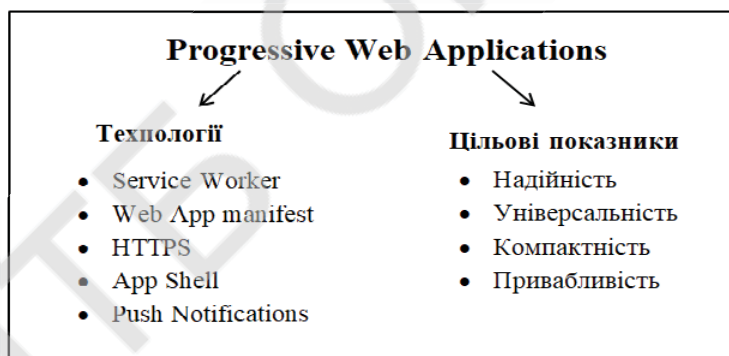


Рис. 1 – Опис технології PWA

Переваги PWA: універсальність – це одночасно і веб-сайт і мобільний додаток; компактність – додатки займають дуже мало місця в пам'яті телефону в порівнянні зі звичайними додатками; доступність до просунутих технологій, так само для PWA доступні і всі функції нативних мобільних додатків: GPS, Push-повідомлення; простота установки та інше [2]. На рис. 2 зображені принципи роботи PWA.

При доступі до веб-сайту, відображаються основні HTML, JavaScript і CSS. При першому відвідуванні веб-сайту на сторінці реєструється Service Worker, який контролює майбутні переходи по сайту. Реєстрація створює новий екземпляр Service Worker і запускає install подію, на яку Service Worker відповідає. Коли Service Worker встановлений, вміст оболонки додатку додається в кеш. Після установки Service Worker контролює майбутні переходи по сайту. Іноді можна вручну активувати нового Service Worker за допомогою інструментів розробника браузерів або програмно за допомогою Api SW.

ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ ДЛЯ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ІНФОРМАЦІЙНИМИ РЕСУРСАМИ	
Сіромля С.Г.	241
ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ОПЕРАТОРОМ ХОЛОДИЛЬНИХ УСТАНОВОК	
Селіванова А.В., Мазурок Т.Л., Селіванов А.П.	242
ПОСТКВАНТОВЕ ШИФРУВАННЯ, БЛОКЧЕЙН, НАВЧАЛЬНІ ТА НАУКОВІ ПРОЦЕСИ	
Кононович І.В.	244
ПРИНЦИПИ ПОБУДОВИ ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЇ	
Владімірова В.Б.	245
ВИКОРИСТАННЯ PWA ТЕХНОЛОГІЇ ПРИ РОЗРОБЦІ КРОСПЛАТФОРМЕННИХ ДОДАТКІВ	
Тройніна А.С.	247
ТЕОРІЯ ГРАНИЧНИХ РЕЖИМІВ РОЗПОВСЮДЖЕННЯ ДЕТОНАЦІЙНИХ ХВИЛЬ В КРУГЛИХ ЦИЛІНДРИЧНИХ ТРУБАХ	
Волков В.Е.	248
ДОСЛІДЖЕННЯ ПРОЦЕСІВ ГОРІННЯ ПАЛИВА В КАМЕРАХ ДВИГУНІВ	
Волков В.Е., Макоєд Н.О.	250
НАУКОВО-МЕТОДИЧНИЙ СУПРОВІД ПРОЦЕСУ ПІДГОТОВКИ МАЙБУТНІХ ІНЖЕНЕРІВ ДО ВИКОРИСТАННЯ НОВІТНІХ ТЕХНОЛОГІЙ	
Лобода Ю.Г.	252
ПРОБЛЕМИ КЕРУВАННЯ ПРОЦЕСОМ ДОКУМЕНТООБІГУ У ЗАКЛАДІ ВИЩОЇ ОСВІТИ	
Волков В.Е., Кириченко В.І.	254
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ОЦІНКИ РИЗИКУ ДЕТОНАЦІЙНОГО ВИБУХУ	
Волков В.Е., Коваленко А.В.	257
ДОСЛІДЖЕННЯ СТІЙКОСТІ ПРОЦЕСІВ ГОРІННЯ З УРАХУВАННЯМ НЕЛІНІЙНИХ ЕФЕКТІВ	
Волков В.Е., Кривченко Ю.В.	258

СЕКЦІЯ «ТЕПЛОФІЗИКА ТА ПРИКЛАДНА ЕКОЛОГІЯ»

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ЦИРКУЛЯЦІЇ ДОМІШОК КОМПРЕСОРНОГО МАСТИЛА В РОБОЧИХ ТІЛАХ ПО КОНТУРУ ХОЛОДИЛЬНОЇ КОМПРЕСОРНОЇ СИСТЕМИ	
Корнієвич С.Г., Нестеров П.С., Желєзний В.П., Семенюк Ю.В.	259
ВПЛИВ ДОМІШОК МОДЕЛЬНОГО КОМПРЕСОРНОГО МАСТИЛА TEG В ХОЛОДОАГЕНТІ RE170 НА ПАРАМЕТРИ ЕФЕКТИВНОСТІ КОМПРЕСОРНОЇ СИСТЕМИ	
Івченко Д.О., Желєзний В.П.	261
ТЕХНОЛОГІЇ ВИКОРИСТАННЯ ЗЕРНОВОГО ПИЛУ НА ПІДПРИЄМСТВАХ ГАЛУЗІ ХЛІБОПРОДУКТІВ	
Заєрклянний М.М., Столевич Т.Б.	264
ПРИНЦИПИ ТЕРМОДИНАМІЧНОГО МОДЕЛЮВАННЯ ТЕПЛОФІЗИЧНИХ ВЛАСТИВОСТЕЙ НАНОФЛЮІДІВ	
Хлієва О.Я., Желєзний В.П., Мотовий І.В.	265

СЕКЦІЯ «КРІОГЕННА ТЕХНІКА»

ПРОМИСЛОВІ УСТАНОВКИ ДЛЯ РОЗДІЛЕННЯ НЕОНОГЕЛІЄВИХ СУМІШЕЙ	
Бондаренко В.Л., Вігуржинська С.Ю., Пилипенко Б.О.	268
АВТОМАТИЗОВАНА УСТАНОВКА ДЛЯ ОТРИМАННЯ КСЕНОНУ ШЛЯХОМ НИЗЬКОТЕМПЕРАТУРНОЇ ДИСТИЛЯЦІЇ	
Бондаренко В.Л., Медушевський Є.Ю., Чигрін А.О., Биканов О.М.	270
ПЕРСПЕКТИВНА СХЕМА ЗРІДЖУВАЧА ВОДНЮ	
Кравченко М.Б.	271
НОВІ ДОСЛІДЖЕННЯ ПОВІТРЯНИХ КОНДЕНСАТОРІВ МАШИН КОМЕРЦІЙНОГО ПРИЗНАЧЕННЯ	
Морозюк Л.І., Соколовська-Єфименко В.В., Гайдук С.В., Мошкатюк А.В.	272
РЕДУКУВАННЯ ПРИРОДНОГО ГАЗУ ВИСОКОГО ТИСКУ У ВИХРОВИХ ТРУБАХ	
Симоненко Ю.М., Бодюл О.С., Тишко Д.П.	274
НЕОНОВІ СИСТЕМИ ОХОЛОДЖЕННЯ В ІНТЕРВАЛІ $T=18...28$ К	
Симоненко Ю.М., Меркулов М.Ю.	275