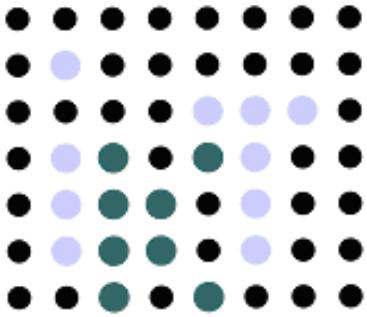
КАФЕДРА ТВЕРДОТІЛЬНОЇ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДВНЗ „УжНУ”

УКРАЇНСЬКЕ ФІЗИЧНЕ ТОВАРИСТВО

АКАДЕМІЯ ТЕХНОЛОГІЧНИХ НАУК УКРАЇНИ

19 грудня 2017

УЖГОРОД



IV НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

"ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ЖИТТІ СТУДЕНТІВ ТА МОЛОДИХ НАУКОВЦІВ ЗАКАРПАТТЯ"

19 грудня 2017 року

ПРОГРАМА І ТЕЗИ

КОНФЕРЕНЦІЇ

УЖГОРОД - 2017

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Морозов А. О. - Почесний голова, д. техн. н., професор, Заслужений діяч науки і техніки України, академік НАН України, академік Міжнародної Академії інформатики, Президент Академії технологічних наук України;
Різак В. М. - Голова, д. фіз-мат. н., професор, завідувач кафедри ТЕІБ, Заслужений діяч науки і техніки України, Голова Закарпатського фізичного товариства;
Студеняк І. П. - д. фіз-мат. н., професор, проректор з наукової роботи ДВНЗ ”УжНУ”, Заслужений діяч науки і техніки України;
Романовський В. М. – полковник, Начальник Управління Державної служби спеціального зв’язку та захисту інформації України в Закарпатській області ;
Повідайчик М. М. - к. ек. н., декан математичного факультету ДВНЗ „УжНУ”;
Повхан І. Ф. - к. техн. н., декан факультету інформаційних технологій ДВНЗ „УжНУ”;
Туряниця І. І. - к. фіз-мат. н., декан інженерно-технічного факультету ДВНЗ „УжНУ”;
Пагіря М. М. – к. фіз.-мат. н., доцент кафедри природничих дисциплін та інформаційних технологій МДУ;
Юркович Н. В. - к. фіз-мат. н., доцент кафедри ТЕІБ ДВНЗ „УжНУ”;
Халус А. – аспірантка УжНУ;
Минда Г. – студентка УжНУ.

ЖУРІ

Морозов А. О. - Почесний голова, д. техн. н., професор, академік НАН України, академік Міжнародної Академії інформатики, Президент Академії технологічних наук України, Заслужений діяч науки і техніки України;
Різак В. М. - Голова, д. фіз-мат. н., професор, завідувач кафедри ТЕІБ, Голова Закарпатського фізичного товариства;
Пагіря М. М. – к. фіз.-мат. н., доцент кафедри природничих дисциплін та інформаційних технологій МДУ;
Млавець Ю. Ю. - к. фіз.-мат. н., заступник декана з наукової роботи математичного факультету УжНУ;
Кут В. І. – к.техн.н., доцент УжНУ;
Сватюк О. Я.- старший викладач УжНУ;
Попович Н. І. - к. фіз-мат. н., доцент УжНУ;
Юркович Н. В. - к. фіз-мат. н., доцент УжНУ;
Чобаль О. І. - к. фіз-мат. н., доцент УжНУ;
Барта А. А. – викладачУжНУ;
Маркевич П. В. – викладач УжНУ;
Мисло Ю. М. – викладач УжНУ;
Каменца Є. - – аспірантУжНУ;
Парлаг В. – аспірант ІЕФ НАН України;
Пірогов О. – аспірант УжНУ;
Халус А. – аспірантка УжНУ;
Минда Г. – студентка УжНУ.

ВСТУПНЕ СЛОВО

Під впливом науково-технічного прогресу імплементуються нові інформаційні технології, які дають унікальні можливості для швидкого розвитку як окремої особистості, так і країни загалом. Повсюдне використання інформаційних ресурсів, які є продуктом інтелектуальної діяльності найбільш кваліфікованої частини працездатного населення, визначають необхідність підготовки в підростаючому поколінні творчого активного резерву. З цієї причини стає актуальною розробка певних методичних підходів до використання засобів нових інформаційних технологій для реалізації ідей розвиваючого навчання, розвитку особистості учня. Як же допомогти поколінню next оцінити безмежні перспективи новітніх інформаційних технологій? Як перетворити підлітків з пасивних споживачів сумнівного розважального контенту на вдумливих творців сучасності? Саме ці та інші актуальні питання стали лейтмотивом цієї науково-практичної конференції.

Науково-практична конференція «Інформаційні технології у житті студентів та молодих науковців Закарпаття» допомагає залучити талановиту молодь до створення нових ІТ продуктів та вдосконалення вже існуючих, а також дає змогу отримати студентам перші гроші за свої наукові розробки.

Наразі передові інновації охоплюють все більше сфер життєдіяльності, сприяючи підвищенню комфорту та гарантуючи стабільну роботу різноманітних сервісів з обслуговування громадян. Маємо шанс налагодити тісніші наукові стосунки з різними вишами України і закордону та підтримувати їх. Такі знайомства створюють змогу спільно шукати гранти, розвивати спільні тематики тощо.

Впенений, що доповіді сприятимуть активній дискусії, в якій буде виражено бачення шляхів розвитку ІТ-технологій, вказано пріоритетних напрямків їх запровадження шляхом об’єднання зусиль усіх зацікавлених сторін.

З повагою,
проректор з наукової роботи ДВНЗ ”УжНУ”,
д.ф.-м.н., проф. **І.П.Студеняк**

ШАНОВНІ УЧАСНИКИ КОНФЕРЕНЦІЇ !

Від імені департаменту освіти та науки облдержадміністрації щиро вітаю Вас на цій надзвичайно актуальній у наш час конференції. Вона стала для вас традиційною, бо тут Ви, студенти, аспіранти, молоді науковці і їх наставники, обмінюєтеся результатами науково-практичних досліджень та досвідом у галузі інноваційних та інформаційно-комунікаційних технологій. Сфера, в якій Ви реалізуєте себе, надзвичайно стрімко розвивається, за нею майбутнє науки і суспільства. Бо ефективність функціонування суспільства багато в чому залежить від кількості та якості інновацій, їхнього змісту, характеру, спрямованості інноваційних процесів.

Облдержадміністрація всіляко підтримує підготовку фахівців у цій галузі та забезпечує розвиток ІТ-технологій у вищих навчальних закладах шляхом запровадження і реалізації довгострокових регіональних програм, зокрема це: «Програма підвищення якості фахової підготовки та кваліфікації фахівців з інформаційної безпеки в Ужгородському національному університеті на 2012 – 2014 роки», «Програма розвитку регіональної вищої освіти на 2013 – 2017 роки» та «Програма розвитку освіти Закарпаття на 2013 – 2022 роки».

Науково-практична конференція «Інформаційні технології у житті студентів та молодих науковців Закарпаття» має на меті підтвердити нагальну необхідність упровадження інформаційно-комунікаційних технологій у сферу вищої освіти як обов`язкову умову переходу до якісного інформаційного суспільства.

Уже традиційно, по завершенні роботи конференції кращі доповіді учасників будуть відзначені пам’ятними призами за фінансової підтримки департаменту освіти та науки облдержадміністрації.

Бажаю всім учасникам конференції нових цікавих знайомств, ідей, проектів та творчої наснаги у своїй діяльності. Впевнена, що будуть активні і плідні дискусії, а матеріали конференції принесуть вагомий внесок у розвиток науки і суспільства.

Головний спеціаліст відділу вищої професійно-технічної освіти
та науки департаменту освіти та науки облдержадміністрації,
канд.фіз.-мат.наук

Ю.Ю.Бабинець

ПРОГРАМА

КОНФЕРЕНЦІЇ

Головуючий: ***Різак В. М.*** - *д. фіз-мат. н., професор, завідувач кафедри ТЕІБ, Голова Закарпатського фізичного товариства;*

Секретар: ***Минда Г. –*** *студентка фізичного факультету.*

09:00 Відкриття конференції - **Різак В.М.**, д. ф.-м. н., професор, завідувач кафедри твердотільної електроніки та інформаційної безпеки ДВНЗ „УжНУ”. Вітальне слово **Смоланки В.І.** - д. мед. н., професора, ректора ДВНЗ ”УжНУ”, **Студеняка І. П.** - д. фіз-мат. н., професора, проректора з наукової роботи ДВНЗ ”УжНУ”, **Бабинця Ю. Ю. –** головного спеціаліста департаменту освіти і науки Закарпатської ОДА.

09:30 Біланич Богдан Віталійович. Використання халькогенідних плівок для виготовлення захисних елементів за технологією електронно- променевої літографії**.**

09:45 Роспопа Петро Михайлович. Система безпровідного керування температурним режимом приміщення на базі технології BLE та термостату.

10:00 Фоменко Ярослава Ярославівна, Кризина Маріанна Сергіївна. Проектування, фізичне підключення та програмне налаштування комп’ютерного кластеру кафедри твердотільної електроніки та інформаційної безпеки УжНУ.

10:15 Гайсак Андрій Іванович. Особливості конфігурації багатосистемних ПК

10:30 Шпонтак Іван Ярославович. Актуальні проблеми кіберзлочинності для сучасної України.

10:45 Фучко Катерина Павлівна. Розробка системи планування ресурсів (ERP-система) для автоматизації обліку успішності студентів.

11:00 Кузнєцов Юрій Олександрович, Пляцко Наталія Володимирівна. Система керування мікрокліматом сушильної камери.

11:15 Калинич Юлінна. Стартап з AR. Анімація для книг.

11:30 Кава брейк.

12:00 Попович Дмитро Петрович. Автоматичний іоноселективний

аналізатор електролітів біологічних розчинів

12:15 Русин Павло Богданович. Створення захищеної корпоративної мережі із застосуванням технологій VPN.

12:30 Повханич Оксана Павлівна. Комп'ютерна система керування гравіювальним верстатом.

12:45 Пішковцій Марія-Ольга Іванівна. Виявлення вразливостей 0-day у Wi-Fi адаптерах.

13:00 Габор Іван, Дулішкович Георгій. Розробка інформаційної системи «Карта діалектів України».

13:15 Кастровська Надія Юріївна. Розробка захищеної мікросервісної архітектури з використання механізмів контейнеризації та overlay мереж як інформаційно-комунікаційної системи.

13:30- Чопей Євген Володимирович. Проблеми захисту соціальних мереж.

13:45- Бабіля Петро Вікторович. Символьне кодування з використанням алгоритмів самоорганізації нейроних мереж Хебба та їх модифікації в системі Auto CAD.

14:00 Ігнатко Марія Іванівна. Впровадження сучасних інформаційно-комунікаційних технологій як запорука інноваційного розвитку агропромислового виробництва України.

14:15 Кравець Євген Володимирович. Проектування, монтаж та конфігурування захищеної мережі IP-телефонії кафедри твердотільної електроніки та інформаційної безпеки.

14:30 Харук Сергій Сергійович. Розробка мобільного додатку Android та всеуніверситетської бази даних успішності студентів для автоматизованого обчислення їх семестрового рейтингу та визначення стипендіатів.

14:45 Єдінак Олександр Вікторович. Розробка інтелектуально-робочої станції на багатоядерних і графічних процесорах для вирішення науково-технічних завдань.

15:00 Шиченко Віталій Васильович. Розробка багатофункціонального сховища персональних даних для Android.

15:15 Деяк Степан Степанович. Розробка централізованого засобу дистанційного навчання для вищої освіти

15:30 Кава брейк

15:45 Буковецький Василь Іванович. Класифікація та обхід текстових версій «CAPTCHA»

16:00 Росоха Сергій Сергійович. ANDROID – додаток для обліку відвідування занять та успішності учнів.

16:15 Ямкова Владіслава Ярославівна. Комплексна система захисту інформації для об'єкта інформаційної діяльності на прикладі державної установи м. Хуст

16:30 Герей Тетяна Мирославівна. Розширення функціональних можливостей і сфер застосування інформаційних систем. Проектування бази даних за допомогою інструмента MySQL Workbench.

16:45 Планчак Олександр Іванович. Фотоіндуковані зміни мікро- і нанотвердості використовуваних у голографічному захисті інформації плівок системи Ge-As-Se.

17:00 Матей Анастасія Олексіївна. Особливості систем захисту інформації на мові програмування Swift на мобільних пристроях IPhone.

17:15 Дурдинець Ярослав Олександрович. Розробка програмного додатку для комплексного моніторингу стану системи на мобільних пристроях під управлінням ОС Android.

17:30 Галас Сергій Сергійович. Розвиток WEB технологій.

17:45 Пухляк Світлана Володимирівна. Створення PWA при розробці електронної комерції з використанням платформи Mobify.

18:00 Кондрат Олександр Олександрович. Моделювання та дослідження наношарів As_x Se_{100-x} як сучасних і перспективних матеріалів для засобів захисту інформації.

18:15 Кейс Владислав Сергійович. Створення антивірусної програми.

18.30 Барта Адальберт Адальбертович. Ковальов Олександр Олександрович, Минда Ганна Юріївна. Моделювання поверхні TiO_2 в квантово-хімічній програмі Quantum Espresso.

18:45 Пирогов Олексій Олександрович. Аналіз можливостей злому RFID систем та розробка захисту.

19.00 Липчей Мар'яна В'ячеславівна. Інформаційна технологія функціонування захищеної системи обміну даними в умовах кібернетичного протиборства.

19.15 Стародубов Дімітар Олексійович, Густі Владислав Володимирович, Хома Петро Петрович. Застосування оптичних захисних елементів (голограм) як ефективного і надійного методу захисту інформації.

19.30 Рокосовик Віталій Олександрович. Розробка сайту кафедри ТЕІБ та системи його захисту.

19.45 Григоревський Віктор Вікторович, Григоревський Станіслав Вікторович. Безпека WEB-ресурсів: XSS і CSRF атаки та методи захисту від них.

20.00 Островка Дмитро Васильович, Єлієшвілі Олена Михайлівна. Бібліотека для відображення тривимірних зображень на основі FBX файлів.

20.15 Урочисте закриття конференції, оголошення переможців, вручення нагород.

ТЕЗИ

КОНФЕРЕНЦІЇ

СИСТЕМА БЕЗПРОВІДНОГО КЕРУВАННЯ ТЕМПЕРАТУРНИМ РЕЖИМОМ ПРИМІЩЕННЯ НА БАЗІ ТЕХНОЛОГІЇ *BLE* ТА ТЕРМОСТАТУ

Роспопа П. М.

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Університетська, 14

За останні 10 років ринок мобільних пристроїв дуже змінився. Пристрої, які колись були доступні лише вузькому колу людей зараз є загальнодоступними і мають набагато більше можливостей ніж їх попередники. Мобільні пристрої стали, як повсякденним робочим інтсрументом, так і засобом розваги. Аналіз сучасних бізнес звітів показав, що кількість різноманітних мобільних пристроїв, які купують, зрівнюється з кількістю куплених ПК.

Bluetooth Low Energy (Bluetooth Smart) – бездротова мережева технологія, яка допомагає повсякденним гаджетам працювати довше, використовуючи при цьому менше енергії. Заснована на недорогих мікросхемах в передавальних пристроях. Використовується для додатків в області охорони здоров'я, фітнесу, систем безпеки.

На сьогоднішній день все більше набувають популярності додатки, які взаємодіють з різними периферійними пристроями по *Bluetooth*. Основне призначення *Bluetooth* – забезпечення економного (з точки зору споживаного струму) і дешевого радіозв'язку між різноманітними типами електронних пристроїв, таких як мобільні телефони та аксесуари до них, портативні та настільні комп'ютери, принтери та інші. Причому, велике значення приділяється компактності електронних компонентів, що дає можливість застосовувати *Bluetooth* у малогабаритних пристроях розміром з наручний годинник.

В даній роботі розроблено програмний додаток, який здійснює взаємодію з програмно-апаратним комплексом *The Smart Radiator Valve*, використовуючи технологію *BLE*.

Загальні характеристики мобільного додатку:

- багатокористувацький режим;
- можливість конфігурування пристрою;
- довільна кількість *Bluetooth* пристроїв;
- збереження даних як локально, так і на сервері;

– створення графіків бажаних температур;
– гнучке налаштування розкладу заданих значень температури по вибраним дням для окремих приміщень;
– керування всіма пристроями одночасно;
– офлайн режим роботи;
– налаштування режимів роботи.

Для реалізації описаних функцій мобільний пристрій забезпечує наступні технічні вимоги:

– операційна система: *iOS 8* і вище;

– модель *iPhone 4S* або вище, *iPad mini* або вище, *iPad (3rd gen)* або вище, *iPod touch (5th gen)* або вище.

Розроблений додаток характеризується економним використанням ресурсів, є інтуїтивно простий у використанні і має звичний дизайн управління програмно-апаратним комплексом.

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. The official website for the Bluetooth wireless technology [Електронний ресурс]. – режим доступу:
https://www.bluetooth.com

2. Core Bluetooth Programming Guide Learn how to build iOS apps and Mac apps that can communicate with Bluetooth Low Energy (BLE) devices [Електронний ресурс]. – режим доступу:
https://developer.apple.com/bluetooth

3. Ultra Low Power Wireless Solutions from NORDIC SEMICONDUCTOR [Електронний ресурс]. – режим доступу:
www.nordicsemi.com

4. Alasdar A. Geolocation in iOS / A. Alasdar – O'Reilly Media, 2012. – 116 с.

5. Alessi P. Professional iOS Database Application Programming, 2nd Edition / P. Alessi – Apress, 2013. – 384 с.

6. Alex H. More iOS 6 Development / H. Alex – Sanoma, 2014. – 689 с.

7. Aftab M. Building Bluetooth Low Energy Systems – Packt, 2017. – 242 с.

8. Bhargava M. IoT Projects with Bluetooth Low Energy – Packt, 2017. – 271 с.

9. Calasdir A. Pro Basic Sensors in iOS / A. Calasdir – Apress, 2011. – 392 с.

10. Davidson R. Getting Started with Bluetooth Low Energy / K. Townsend – O'Reilly Media, 2015. – 180 с.

11. Gupta N. Inside Bluetooth Low Energy, Second Edition (Mobile Communications) – Artech House, 2016. – 458 с.

12. Heydon R. Bluetooth Low Energy: The Developer's Handbook – Prentice Hall, 2012. – 368 с.

БЕЗПЕКА WEB-РЕСУРСІВ: XSS І CSRF АТАКИ ТА МЕТОДИ ЗАХИСТУ ВІД НИХ.

Григоревський В.В., Григоревський С.В
ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54

CSRF / XSRF (Cross Site Request Forgery – «міжсайтова підробка запиту», також відомий як XSRF) – це вид уразливості, що дозволяє використовувати недоліки HTTP-протоколу. Найбільш частими CSRF атаками є атаки з використанням тегу HTML <IMG> тегу або Javascript об'єкта image. Таким чином при завантаженні сторінки здійснюється запит, виконується шкідливий код. Ілюстрація:
IMG SRC

```
<img src="http://hacker_site/?command">
```

Зловмисники працюють за такою схемою:

1. Посилання на шкідливий сайт встановлюється на сторінці, що користується довірою у користувача.
2. При переході по шкідливому посиланні виконується скрипт, який зберігає особисті дані користувача (паролі, платіжні дані і т.д.), або відправляє СПАМ повідомлення від особи користувача, або змінює доступ до облікового запису користувача для отримання повного контролю над ним.

XSS атака (Cross Site Scripting) є атакою на вразливість, що дозволяє впровадити в згенеровану сервером HTML-сторінку якийсь довільний код і передавати його як значення змінної, фільтрація по якій не працює, тобто сервер не перевіряє дану змінну на наявність в ній заборонених знаків -, <,>, ', ". Значення цієї змінної передається від згенерованої HTML-сторінки на сервер в скрипт шляхом відправлення запиту. PHP-скрипт у відповідь на даний запит генерує HTML-сторінку, в якій відображаються значення потрібних хакеру змінних, і відправляє дану сторінку на браузер хакера.

- Для запобігання проведення XSS атак використовують такі методи і засоби захисту веб сайтів:

- Заборонити включення безпосередньо параметрів $ _GET, $ _POST, $ _COOKIE в згенеровану HTML-сторінку. Рекомендується використовувати альтернативні функції і параметри.
- Заборонити завантаження довільних файлів на сервер, щоб уникнути завантаження шкідливих скриптів. Зокрема, рекомендується заборонити завантаження на сервер файлів різних типів скриптів і HTML-сторінок.
- Всі завантажені файли зберігати в базі даних, а не в файловій системі. Структури даних це не порушує (навіть навпаки), а проблем може бути значно менше.
- При розширенні функціональності сайту, зростає можливість проведення XSS атак, тому розширення слід проводити з обережністю і регулярним тестуванням.

Також щоб якомога краще захистити Web- ресурс , тестувальники проводять тестування безпеки (Security Testing). Для того щоб протестувати, фахівці з тестування користуються різними інструментами (Tools) зокрема proxy - серверами.

Fiddler - проксі, який працює з трафіком між вашим комп'ютером і віддаленим сервером, і дозволяє інспектувати і міняти його. Fiddler можна розширювати за допомогою скриптів на мові JScript.NET.
Тестувальник може перехвачувати запити, і міняти їх. Також імітувати відповіді від сервера.

Таким чином, тестовими випадками можна швидко і якісно знайти помилки в системі (або пересвідчитись в тому що їх нема) , і цим забезпечити високу якість продукту.

КЛАСИФІКАЦІЯ ТА ОБХІД ТЕКСТОВИХ ВЕРСІЙ «CAPTCHA»

Буковецький В. І., Васильєв О. В.

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54

В життєвому циклі багатьох проектів рано чи пізно наступає момент зустрічі з програмами автоматичного збору інформації, такі програми не тільки можуть скопіювати цінну інформацію, але й сповільнити доступ до ресурсу, зайнявши весь доступний серверу канал.

Для захисту від автоматизованих запитів до сайту зазвичай використовують системи CAPTCHA (CompletelyAutomatedPublicTuringtesttotellComputersandHumansApart) — комп'ютерний тест типу виклик-відповідь, який використовується для того, щоб визначити, хто використовує систему — робот чи людина.

Зазвичай такі тести являють собою зображення з певним коротким текстом (1-2 слова), який модифіковано (спотворено, додано шум, сторонні елементи) таким чином, аби задача розпізнавання була посильною для людини, але важкою для обходу системи OCR.

Метою дослідження є демонстрація та опис практичної методики обходу однієї з варіацій тесту CAPTCHA.

В результаті виконання роботи було створено програму, яка вирішує задачу CAPTCHA одного з сайтів, який використовує власну реалізацію алгоритму. В програмі використовуються лише прості техніки маніпуляції зображнням та найпростіша імплементація перцептрону.

З роботи можна зробити висновки, що технології розвиваються і старі методи захисту від автоматичних запитів вже не є такі ефективні, тому слід якнайшвидше відмовитись від використання тестів з використанням спотвореного тексту, те перейти на більш складні задачі, які ще не є посильними для сучасних алгоритмів та передових технологій нейронних мереж.

КІБЕРБЕЗПЕКА ПРОЕКТУВАННЯ БАЗИ ДАНИХ ЗА ДОПОМОГОЮ ІНСТРУМЕНТА MYSQL WORKBENCH.

Герей Т. М.
ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54

Ми живемо в епоху бурхливого розвитку науки і техніки. Одночасно з цим постійно зростає обсяг існуючої інформації. Інформація–відомості про об'єкти та явища навколишнього середовища, їх параметри, властивості, стан. Системи, призначені для збирання, пошуку, зберігання, опрацювання інформації називаються інформаційними системами. До них належить як звична нам техніка (телевізор, комп'ютер, смартфон) так і ми самі виступаємо в ролі інформаційної системи – як окремий індивід і як певна соціальна група.

Бази даних також можна розглядати як інформаційну систему. У загальному випадку база даних – це впорядкований набір даних. У сучасних інформаційних системах для роботи з базами даних використовують системи керування базами даних – програмне забезпечення, яке дозволяє створювати бази даних, керувати, маніпулювати ними. Однією з найпоширеніший СКБД є MySQL. Це компактний багатопотоковий сервер баз даних. Інструментом для візуального проектування баз даних є програма MySQL Workbench.Однією з переваг є те, що вона дозволяє представити модель бази даних у графічному вигляді – EER-діаграмі (діаграма "сутність-зв'язок").Цей інструмент також є дуже корисним для веб-програмістів, тому що дозволяє швидко створювати бази даних, SQL-запити, синхронізувати їх із віддаленим сервером.

Як приклад, мною була створена інформаційно-комунікаційна система інтернет-маркету. Вона складається із сайту магазину, з яким взаємодіє відвідувач та серверної частини, яка включає в себе базу даних товарів, створену за допомогою MySQL Workbench.

РОЗРОБКА ПРОГРАМНОГО ДОДАТКУ ДЛЯ КОМПЛЕКСНОГО МОНІТОРИНГУ СТАНУ СИСТЕМИ НА МОБІЛЬНИХ ПРИСТРОЯХ ПІД УПРАВЛІННЯМ ОС ANDROID

Дурдинець Я.О.

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54

Мобільні пристрої стали невід`ємною частиною нашого життя тому важливо, щоб стан роботи цього пристрою був завжди задовільний. Для підтримки цього стану використовуються утиліти, які дають можливість діагностувати й усувати проблеми і забезпечувати ефективну роботу системи.

Метою моєї роботи є розробка програмного продукту, який аналізує стан системи і при необхідності повідомляє користувача про нестабільну роботу його мобільного пристрою. Для забезпечння комплексного моніторингу стану системи програмний додаток буде включати в себе декілька функцій: по перше - це аналіз споживання заряду батареї. За допомогою Android SDK будуть отримуватись дані про зміну заряду і відображатись користувачеві в вигляді діаграми і по друге - аудит файлової системи для очищення від тимчасових та застарілих файлів.

Іншою функцією розробленого программного додатку буде блокування СМС повідомлень та вхідних дзвінків. Номер який доданий користувачем до списку заблокованих, буде перехоплюватись BroadcastReceiver менеджером та пройшовши певну фільтрацію блокуватиметься.

Для того щоб користувач завжди міг слідкувати за станом системи, навіть коли телефон знаходиться в заблокованому стані, в додаток будуть додані “Push notification”.

Додаток розроблятиметься на основі мови програмування JAVA з використанням proguard бібліотеки для обфускації коду додатку, щоб мінімізувати можливість злому та отримання коду зловмисником.

РОЗРОБКА ІНТЕЛЕКТУАЛЬНО-ПАРАЛЕЛЬНОЇ РОБОЧОЇ СТАНЦІЇ НА БАГАТОЯДЕРНИХ І ГРАФІЧНИХ ПРОЦЕСОРАХ ДЛЯ ВИРІШЕННЯ НАУКОВО-ТЕХНІЧНИХ ЗАВДАНЬ

Єдінак О. В.

ДВНЗ «Ужгородський національний університет»
88000, м. Ужгород, вул.. Волошина, 54

Метою даної роботи є створення дослідного зразка знання орієнтованої інтелектуальної паралельної робочої станції MIMD архітектури (CPU) з графічними процесорами SIMD-архітектури (GPU), яка в автоматичному режимі досліджує властивості комп'ютерної моделі задачі, будує алгоритм, формує топологію, створює код паралельних обчислень, вирішує завдання і оцінює його достовірність з теоретичною продуктивністю не менше п'яти терафлопс (TFLOPS).

Інтелектуальна станція включає хост-систему і обчислювальний блок.

Хост-система здійснює:

- управління використанням многопроцессорного обчислювального ресурсу;
- загальносистемний моніторинг;
- спілкування з термінальними мережами користувачів;

Обчислювальний блок здійснює вирішення задачі з паралельною організацією обчислень, є однорідною структурою, яка складається з безлічі вузлів (з CPU, GPU, власної оперативної і дискової пам'ятті), об'єднаних комунікаційним середовищем межпроцесорної взаємодії.

Структура і склад дослідного зразка інтелектуальної паралельної робочої станції: 4 обчислювальних вузла (2 процесора Xeon 5600, 24 Gb оперативної пам'яті, 500 Gb дискової пам'яті RAID1, 2 адаптера з графічними процесорами); дискове сховище від 4ТБ. Комунікаційне середовище: Gigabit Ethernet; InfiniBand QDR; IPMI.

Структура і склад програмного забезпечення інтелектуальної паралельної робочої станції. Операційне

середовище: операційна система Linux (Windows); компілятори C / C ++, Фортран, CUDA; середовище міжпроцесорної взаємодії MPI; системний програмний монітор.

Операційне середовище забезпечує:

- формування завдання і запуск паралельного завдання на обраних обчислювальних вузлах;
- моніторинг інтелектуального комп'ютера і виконання завдань;
- збереження і візуалізація протоколів паралельних розрахунків;
- запуск програми (виконуваного коду програми);
- розробку паралельних програм;
- адміністрування доступних користувачеві частин розподіленої файлової системи.

Інтелектуальне чисельне програмне забезпечення:

• бібліотека інтелектуальних програм дослідження і вирішення базових завдань обчислювальної математики;

• інтелектуальний програмний засіб автоматичного дослідження і вирішення базових завдань обчислювальної математики;

• інтелектуальне прикладне програмне забезпечення для вирішення науково-технічних завдань з різних предметних областей.

Складові частини інтелектуального програмного засобу по кожному класу: діалогова система, бібліотека функціональних модулів, плануючий/керуючий блок, блок пояснень.

Інтелектуальну паралельну робочу станцію доцільно використовувати для завдань:

- математичного моделювання складних процесів, явищ, об'єктів і систем;
- розрахунку міцності конструкцій;
- аеро- і гідродинамічні розрахунки при створенні тренажерів управління складними процесами об'єктів сучасної техніки;
- вирішення складних науково-технічних завдань з наближено заданими вихідними даними;
- адаптації на гібридну архітектуру програмних комплексів вирішення складних завдань, створених раніше для однопроцесорних комп'ютерів, в ході якої переклад завдання з мови користувача в задачку і переклад рішення математичної задачі на мову користувача залишаються незмінними, а рішення математичної завдання замінюється на програми вирішення з паралельною організацією обчислень.

РОЗРОБКА ЗАХИЩЕНОЇ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ З ВИКОРИСТАННЯ МЕХАНІЗМІВ КОНТЕЙНЕРИЗАЦІЇ ТА OVERLAY МЕРЕЖ ЯК ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ.

Кастровська Н.Ю.

ДВНЗ «Ужгородський національний університет»
88000, м. Ужгород, вул.. Волошина, 54

Щодня людство використовує як мережу інтернет так і корпоративні мережі для передавання, зберігання та оброблення терабайтів даних . І саме велика кількість інформації спонукає до пошуку методів оптимізації та прискорення процесів необхідних для її якісного використання.

Одним із засобів оптимізаціє є використання механізмів контейнеризації та Overlay мереж як інформаційно-комунікаційних систем, а саме програмне забезпечення для операційної системи Linux – Docker.

Docker — інструментарій для управління ізольованими Linux-контейнерами. Docker доповнює інструментарій LXC більш високорівневим API, що дозволяє керувати контейнерами на рівні ізоляції окремих процесів. Зокрема, Docker дозволяє не переймаючись вмістом контейнера запускати довільні процеси в режимі ізоляції і потім переносити і клонувати сформовані для даних процесів контейнери на інші сервери, беручи на себе всю роботу зі створення, обслуговування і підтримки контейнерів.

Docker суттєво прискорює розробку та цикли розгортання тим самим дозволяючи видавати готовий код в неймовірно короткі терміни. Але ціною швидкості у даному випадку є безпека. Тому перед використання даної системи слід ознайомитися з «дірками» у захисті та тим як їх усунути. В цілому можна виділити такі основні недоліки: достовірність образу, зайві повноваження, безпека системи, обмеження використання ресурсів, велика область для атак, вихід за межі Docker-контейнера, уразливість в образах контейнерів.

Під час виконання даної роботи я зробила спробу розробити програму, яка має вирішувати зазначені вище вразливості, що виникають при застосуванні механізмів контейнеризації та Overlay мереж.

МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ НАНОШАРІВ AS_XSE_{100-X} ЯК СУЧАСНИХ І ПЕРСПЕКТИВНИХ МАТЕРІАЛІВ ДЛЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

Кондрат О.О.

Національний університет «Львівська політехніка»,
Львів 79013, вул. С. Бандери, 12

Аморфні халькогеніди є перспективними матеріалами для застосування в нано- та оптоелектроніці завдяки структурним, електронним та оптичним властивостям у широкому спектральному діапазоні. Аморфні плівки системи As_xSe_{100-x} в даний час представляють інтерес як матеріали для оптоелектронних пристроїв, а також оптичного зберігання інформації. У халькогенідних стеклах під дією лазерного випромінювання відбуваються зміни як властивостей, так і структури. Ці зміни можуть бути незворотними, метастабільними або спостерігатися тільки під час освітлення. Для дослідження і опису структури некристалічних халькогенідів на нанорівні використовувалися численні експериментальні методи, зокрема традиційні методи дифракції, непружного та комбінаційного розсіювання. Крім того, для інтерпретації експериментальних результатів застосовується моделювання структури, зокрема методами молекулярної динаміки та розрахунками з перших принципів.

В даній роботі всі розрахунки структури наношарів As_xSe_{100-x} виконувалися за допомогою програми Gaussian-09. Для розрахунків було використано обмін Слетера та кореляції функціонала Воско, Вілка і Нусайра разом з посиленою кореляцією Даннінга, що містить подвійний зета-базисний набір (aug-cc-pVDZ). Розрахунки енергії МО були виконані на повністю оптимізованих структурах за допомогою алгоритму оптимізації Берні. Таким чином, були розраховані енергетичні діаграми молекулярних орбіта лей різнихструктурних одиниць та виділені лише електронні стани центральних атомів.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ФУНКЦІОНУВАННЯ ЗАХИЩЕНОЇ СИСТЕМИ ОБМІНУ ДАНИМИ В УМОВАХ КІБЕРНЕТИЧНОГО ПРОТИБОРСТВА

Липчей М. В.
ДВНЗ „Ужгородський національнийуніверситет”
88000, Ужгород, вул. Волошина, 54

Сенсорні мережі є єдиною бездротовою технологією, за допомогою якої можна вирішити завдання інформаційної взаємодії в ІТС, спостереження і контролю, за умов критичної зміни параметрів функціонування мережі, зовнішнього та внутрішнього середовища.

На відміну від мереж із ієрархічною структурою і централізованим управлінням, однорангові мережі без інфраструктури складаються з однотипних вузлів, де кожен вузол має комплексом програмно-апаратних засобів, що дозволяють організувати передачу даних від джерела до одержувача безпосередньо при фізичному наявності такого шляху і тим самим розподілити навантаження на мережу і підвищити сумарну пропускну здатність мережі. Передача даних від одного абонента до іншого може відбуватися, навіть у випадку якщо ці вузли знаходяться поза зоною прямої радіовидимості. У цих випадках пакети даних цих абонентів ретранслюються іншими вузлами мережі, які мають зв'язок з кореспондуючими абонентами. Мережі з багаторазової ретрансляцією називаються багатопрольотними або багатоскачковими (multihop). При розробці таких мереж основ-ними проблемами є маршрутизація пакетів від вузла джерела до вузла одержувачу, масштабованість мереж, адресація кінцевих пристроїв, підтримання зв'язності в умовах змінної топології.

Метою мого дослідження є розробка інформаційної технології функціонування захищеної системи обміну даними в умовах кібернетичного протиборства, як сенсорної мережі на базі протоколу ближнього радіозв’язку 802.15.4/ZigBee, що дозволяє створювати самоорганізуючі відмовостійкігарантоздатні ІТС за умов оптимального управління ресурсами в умовах конфлікту та невизначеностей. Сенсорні мережі є єдиною бездротовою

технологією, за допомогою якої можна вирішити завдання інформаційної взаємодії в ІТС, спостереження і контролю, за умов критичної зміни параметрів функціонування мережі, зовнішнього та внутрішнього середовища.

Актуальність даного дослідження обумовлена тим, що переважна більшість наземних мобільних бездротових мереж зв'язку мають фіксовану інфраструктуру, яка включає стаціонарні (AdHoc) та мобільні (MANET) абоненти, з’єднані між собою за допомогою каналів передачі даних і функціонують в умовах конфлікту і невизначеностей в зовнішньому і внутрішньому середовищі ІТС.

При проектуванні та експлуатації сенсорних мереж основним завданням є вирішення проблеми забезпечення гарантоздатності, яка в значній мірі визначається розвиненістю механізму їх управління. Сучасна система управління об'єднує ресурси сенсорної мережі та програмні засоби в єдине ціле і визначає її гарантоздатність. Незважаючи на те, що постійно розробляються нові апаратні та програмні засоби для організації процесів інформаційної взаємо- дії елементів обчислювальних систем і сенсорних мереж, відповідні інформаційні технології ефективного управління такими системами і мережами на поточний час розвинені недостатньо.

ОСОБЛИВОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА МОВІ ПРОГРАМУВАННЯ SWIFT НА МОБІЛЬНИХ ПРИСТРОЯХ IPHONE.

Матей А.О.
ДВНЗ „Ужгородський національнийуніверситет”
88000, Ужгород, вул. Волошина, 54

Робота присвячена особливостям систем захисту інформації на мові програмування Swift на мобільних пристроях IPhone. Метою роботи є демонстрація головних особливостей мови програмування Swift на основі прикладів мобільних додатків. В роботі розглянуто історію розробки та перспективи застосування даної мови програмування. А також наведено приклад створення інформаційних систем в БІКС.

Swift -багатопарадігмова компільована мова програмування, розроблена компанією Apple для того, щоб співіснувати з Objective C і бути стійкою до помилкового коду. Swift була представлена на конференції розробників WWDC 2014 Мова побудована з LLVM компілятор, включеного в Xcode 6 beta.

Вже тепер Swiftє популярною, а з часом кількість її прихильників лише зросте, оскільки вона має багато переваг. Основними перспективами застосування є:

- Для людини Swift більш читабельна мова, ніж Objective-C:
- Swift - легше підтримувати:
- Swift – безпечніша мова:
- Незалежне управління пам'яттю:
- Swift вимагає меншу кількість коду.

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ PWAПРИ РОЗРОБЦІ ЕЛЕКТРОННОЇ КОМЕРЦІЇ НА ПРИКЛАДІ ПЛАТФОРМИ MOBIFY

Пухляк С. В.

ДВНЗ „Ужгородський національний університет”
88000, Ужгород, вул. Волошина, 54

Електронна комерція є невід’ємною частиною розвитку будь-якого бізнесу. За допомогою інтернет магазинів власники можуть пропонувати значно більшу кількість товарів та забезпечити покупця більшим обсягом інформацію необхідної для покупки. З розвитком популярності інтернет магазинів, також і розвиваються технології їх виробництва. Однією з найсучасніших технології є технологія ProgressiveWebApps (PWA).

PWA – це технологія створення мобільних сайтів, за допомогою якої користувач має можливість працювати з сайтом, як із звичайним додатком. Він має можливість скачати його ярлик відразу із браузера на робочий стіл, незалежно від розміру екрана та інших специфікацій пристрою, а також можливість перегляду в автономному режимі відвіданих попередньо сторінок.

Метою мого дослідження є методологія створення PWA при розробці електронної комерції з використанням платформи Mobify, підґрунтям для якого використовується Merlin’sPotionsсайт.

В результаті мого дослідження можна зробити такий висновок.

Платформа Mobify є одним із кращих методів для створення PWA. Вона надає можливість використовувати готові компоненти, картридж для роботи в автономному режимі та різні варіанти витягування даних, а саме:

- витягування вмісту безпосередньо із веб-сайту за допомогою селекторів;
- використанняApplication Programming Interface (API)

При виборі між цими технологіями обов’язково слід звернути увагу, що привитягуванні вмісту безпосередньо із веб-сайту за допомогою селекторів -потрібно переконатись, що на десктопному веб-сайті не будуть змінюватись селектори до яких прив’язується PWA. Більш надійним способом є використання API, що надає можливість незалежного функціонування від десктопноговеб-сайту.

ANDROID -ДОДАТОК ДЛЯ ОБЛІКУ ВІДВІДУВАННЯ ЗАНЯТЬ ТА УСПІШНОСТІ УЧНІВ

Росоха С. С.

ДВНЗ „Ужгородський національний університет”
88000, Ужгород, вул. Волошина, 54

Прогули, запізнення, відсутність учнів на заняттях - це проблема кожного навчального закладу. Такі речі ускладнюють навчальний процес, що надалі позначається на загальних показниках успішності. Істотні зміни в інформаційній сфері діяльності людини призводять до суттєвого зниження ефективності застарілих підходів до контролю відвідуваності занять та успішності учнів. Саме тому, сьогодні є доцільною розробка спеціальної системи, яка дозволить автоматизувати процесс обліку відвідування та успішності учнів, зробити його швидшим, зручнішим та надійнішим. Така система, дозволить своєчасно виявляти проблеми з безпричинними пропусками занять та успішності учня. Крім того, такий засіб надаватиме можливість батькам безпосередньо стежити за відвідуванням та результатами успішності своїх дітей.

На сьогоднішній день уже існує достатньо велика кількість веб-орієнтованих продуктів для контролю відвідуваності та успішності, тому основним предметом даної роботи є розробка програмного продукту для мобільних платформ, який надаватиме зручні засоби для контролю та інтегруватиметься із аналогічними веб-орієнтованими системами.

Метою роботи є розробка Android-додатку для обліку відвідування занятьта успішності учнів із можливістю інтеграції із веб-орієнтованим аналогом. Для створення додатку необхідно:

- Аналіз предметної області «Облік відвідуваності та успішності учнів»
- Розробка архітектури програмної системи
- Проектування структури бази даних
- Програмна реалізація
- Тестування та дослідна експлуатація

Більшість навчальних закладів зацікавлені у впровадженні нових технологій як у навчальний так і у виховний процеси, тому

розробка Android-додатку для обліку відвідування занять та успішностіучнів є на даний час актуальною.

СТВОРЕННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ ІЗ ЗАСТОСУВАННЯМ ТЕХНОЛОГІЙ VPN

Русин П. Б.

ДВНЗ „Ужгородський національний університет”
88000, Ужгород, вул. Волошина, 54

Корпоративні комп'ютерні мережі є невід'ємною частиною сучасних компаній. За допомогою таких мереж можна оперативно і безпечно передавати і отримувати інформацію. Вони забезпечують зв'язок між комп'ютерами одного підприємства, розташовані в межах одного будинку або географічно розподіленими.

Задача реалізації корпоративної мережі компанії в межах одного будинкуможе бути вирішена порівняно легко. Однак на сьогодні інфраструктура компаній має географічно розподілені відділення самого підприємства. Реалізація захищеної корпоративної мережі в такому випадку завдання більш складної плану. У таких випадках часто використовуються VPN технології.

При наявності зв'язку між корпоративною локальною мережею та мережею Інтернет виникають загрози інформаційної безпеки двох типів:

- несанкціонований доступ до ресурсів локальної мережі через вхід
- несанкціонований доступ до інформації при передачі через відкриту мережу Інтернет

Метою мого дослідження є порівняння різних способів створення VPN та методів реалізації захищеності приватної мережі.

Для досягнення мети яорендував сервер в Нідерландах, написав скрипт, який реалізує VPN протоколи PPTP, L2TP/IPSec, SSTP, IKEv2 та OpenVPN.

В результаті мого дослідження можна зробити такий висновок.

Ніколи не вибирайте PPTP . Лише, якщо у вас нема альтернативи. Використовуючи цей протокол, виконуйте в мережі лише ті дії, які не вимагають безпеки або захищеності.

Використовуйте L2TP / IPsec, коли вам потрібно. Наприклад, на пристроях iOS, які не працюють з іншими популярними методами, які можуть бути швидшими та безпечнішими.

SSTP є гарною альтернативою для двох пристроїв Windows, яким потрібна сильна захищеність.

IKEv2 - це найновіша та найдосконаліша **пропозиція,** яка ідеально підходить для нових мобільних пристроїв Windows, оскільки не **перестає**захищати VPN-зв'язок під час перемикання між Wi-Fi мережею або мобільними з'єднаннями.

Якщо ви сумніваєтесь, або якщо ви не можете використовувати ці протоколи, завжди можете використовувати OpenVPN. Він поєднує в собі найкраще з усіх категорій і широко доступний на будь-якому пристрої або платформі.Але OpenVPN вимагає встановлення додаткового програмного забезпечення в Windows, Linux, Mac, Android і не працює в iOS.

Плюси використання свого персонального сервера:

- стабільна швидкість;
- відсутність сусідів на IP-адресі;
- Шанованим хостам більше довіри, ніж більшості VPN-сервісів.

Мінуси свого сервера:

- налаштуванняпотребує технічних навичок;
- необхідно стежити за виходом патчів безпеки та оперативно їх застосовувати, щоб сервер не хакнули.

Вибираючи провайдера для побудови та обслуговування корпоративної IP VPN-мережі, важливо бути впевненим у стабільності зв'язку, безпеки даних, що передаються і швидкості вирішення тих чи інших технічних проблем. Думаю, це основні вимоги, до яких слід додати фактор репутації. Тільки компанії, які мають що втрачати, справді займаються своїми клієнтами.

ЗАСТОСУВАННЯ ОПТИЧНИХ ЗАХИСНИХ ЕЛЕМЕНТІВ (ГОЛОГРАМ) ЯК ЕФЕКТИВНОГО І НАДІЙНОГО МЕТОДУ ЗАХИСТУ ІНФОРМАЦІЇ

Стародубов Д.О., Густі В.В.,Хома П.П.

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54

Метою роботи було створення додатку, для безпечного збереження інформації, методом кодування зображення в голограму, з подальшою можливістю відновити інформацію без будь яких її втрат.

Особливістю голографії є одержання видимого образу предмета, який має всі ознаки оригіналу. Адже гологра́фія (від грецького *Ὅλος—holos* — повний + *γραφή—graphe* — запис) — набір технологій для точного запису, відтворення і переформатування хвильових полів.При цьому досягається повна ілюзія присутності предмета.

Для написання додатку використовувалася об’єктно-орієнтована мова програмування Delphi та IDEEmbarcaderoDelphi.

Додаток представляє собою кодування та декодування голографічного зображення, тобто кодування графічного повідомлення відбувається за допомогою голограм. Таким чином - це ефективний спосіб уникнути небажаної втрати інформації.

Метою нашого дослідження є методологія кодування зображення в форматі .bmp в голограму з подальшою можливістю декодування даного зображення зі збереженням оригінальності (або з незначним відхиленням від оригіналу).

Нами було вирішено використовувати Delphi та IDEEmbarcaderoDelphi, адже вони надають можливість використати готові елементи інтерфейсу.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ НА ПРИКЛАДІ ДЕРЖАВНОЇ УСТАНОВИ М. ХУСТ

Ямкова В.Я.

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54

На сьогодні проблема захисту ОІД стає все гострішою і необхідною до розв'язання. Зараз, в період переходу з паперових архівів до електронних баз даних, захист інформації стає дедалі більш важливим і необхідним для комерційних об'єктів та державних структур.

Водночас зі створенням нових продуктів для збереження, обробки та пересилання інформації, з'являються нові методи несанкціонованого доступу до неї.

Тому створення та своєчасне оновлення КСЗІ є актуальним сьогодні, бо дозволяє забезпечити надійний захист цінної комерційної інформації та державної таємниці.

Методика

Під час створення комплексної системи захисту інформації (КСЗІ) для об'єкта інформаційної діяльності (ОІД) використовувалось програмне забезпечення побудови схем для моделі загроз, а саме проектувався ситуаційний та генеральний плани
.

На основі міжнародних та державних стандартів здійснювалась підготовка необхідної документації до затвердження відповідними органами державної влади.

Також на прикладі роботи державної установи, а саме керування робочого процесу, розмежування доступу персоналу до інформації, створювався організаційний захист на ОІД.

На основі дослідження нових технологій захисту інформації був розрахований кошторис обладнання по КСЗІ та розроблені рекомендації по надійному розміщенню їх в будівлі за можливими каналами витоку інформації.

Висновки

Комплексна система захисту інформації (КСЗІ) є сукупністю організаційних і технічних заходів, апаратних і програмних засобів, які забезпечують захист інформації в інформаційно-телекомунікаційних системах.

Захист інформації в сучасних умовах стає все більш складним до виконання. Це обумовлено рядом обставин : масове розповсюдження засобів обчислювальної техніки та їх доступність; стрімкий розвиток технологій; ускладнення шифрувальних технологій; необхідність захисту не тільки державної і військової таємниці, а також, комерційної і фінансової та промислової таємниці; створення нових можливостей несанкціонованих дій над інформацією.

ПРОЕКТУВАННЯ, ФІЗИЧНЕ ПІДКЛЮЧЕННЯ ТА ПРОГРАМНЕ НАЛАШТУВАННЯ КОМП'ЮТЕРНОГО КЛАСТЕРУ КАФЕДРИ ТВЕРДОТІЛЬНОЇ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УЖНУ

Фоменко Я. Я., Кризина М. С.

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54

Комп'ютерний кластер – це група з двох або більше серверів, що діють спільно для забезпечення безвідмовної роботи набору додатків або служб і сприймаються клієнтом як єдиний елемент. Вузли кластера об'єднуються між собою за допомогою системних мережевих засобів, спільно використовуваних розділених ресурсів і серверного програмного забезпечення.

Основна мета використання кластера — забезпечення високої доступності бази даних. Використання кластера серверів баз даних може допомогти запобігти недоступності даних через вихід з ладу сервера, викликаного збоєм у програмному забезпеченні, необхідністю виконання операцій з обслуговування сервера або через втрату мережного з'єднання з сервером. Однак кластер не гарантує, що ніколи не відбудеться відмова сервера, він допомагає зменшувати число виходів з ладу і надає адміністраторам бази даних і сервера можливості вивести сервер зі стану відмови без втрат.

Актуальність кластерного підходу для організації внутрішньої мережі кафедри зумовлена такими перевагами, а саме:

- високий рівень готовності – якщо відбувається збій служби або додатку на якомусь об'єкті кластера, то кластерне програмне забезпечення дозволяє перезапустити цей додаток на іншому сервері. Користувачі при цьому помітять короткочасну затримку при проведенні якої-небудь операції або взагалі не побачать серверного збою.
- масштабність – для прикладних програм, що працюють в кластері, додавання серверів до кластеру означає збільшення можливостей: відказостійкість, розподіл навантаження і т. д.

- керування – адміністратори, використовуючи єдиний інтерфейс, можуть керувати додатками та службами, встановлювати реакцію на збій у вузлі кластера, розподіляти та знімати навантаження серед вузлів для проведення профілактичних робіт.

Для створення кластеру ми використовували таке обладнання:

- база даних (HP ProLiant DL380 G4 Packaged Cluster with MSA1000 G2);
- сервери (HP ProLiant DL380 G4);
- кабелі для з'єднання (Ethernet RJ-45, SCSI);
- комутатор (Cisco Catalyst);
- програмне забезпечення (Windows server 2003 Enterprise Edition)

Методика створення комп'ютерного кластеру включає 3 основні етапи. Першим, з яких є проектування, другим є фізичне підключення та завершальним – програмне налаштування. Перед початком роботи потрібно вирішити для яких цілей буде використовуватися кластер. У нашому випадку це відмовостійка система для обміну даними з можливістю розширення спектру дій. Першим кроком є встановлення програмного забезпечення Microsoft Windows 2003 Server Enterprise Edition на всі вузли кластера. Другим кроком є мережеві налаштування, створення Private Cluster та Public Cluster мереж для обміну даними. Підготовка жорстких дисків та бази даних, їхнє форматування для подальшої роботи. Використання різних служб і менеджерів для надання прав доступу користування ресурсів серверів, створення адміністратора та користувачів. Наступна дія – це перевірка правильності роботи та функціонування всієї системи.

Отже, ми розгорнули відмовостійкий кластер, систему, яка надає доступ до користування даними всім існуючим користувачам. Цей кластер, як правило, складається з чотирьох вузлів, що використовують загальний дисковий ресурс для обміну даними. Цей ресурс також називають кворум-пристроєм (quorum). Кластер містить два різних типи мереж: приватна мережа, яка використовується для підтримки з'єднань між вузлами кластера, і мережу загального користування (локальна мережа), яка використовується клієнтами кластера для під'єднання до служб у цьому кластері. Оскільки з'єднання між вузлами кластера – це потенційна точка відмови, воно завжди має передбачати надмірність. У разі, коли використовуються два мережевих інтерфейси, то при відмові одного з них адміністратор зможе без особливих зусиль переключитися на використання другого.

До того ж використання двох інтерфейсів збільшує швидкість обміну даними і в кінцевому рахунку збільшує швидкість роботи всього кластера в цілому.

КОМП'ЮТЕРНА СИСТЕМА КЕРУВАННЯ ГРАВІЮВАЛЬНИМ ВЕРСТАТОМ

Повханич О. П.
ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Університетська, 14

Автоматизація вважається головним, найбільш перспективним напрямком у розвитку промислового виробництва. Завдяки звільненню людини від особистої участі у виробничих процесах, а також високої концентрації основних операцій істотно поліпшуються умови праці й економічні показники виробництва.

Основні результати

Комп'ютерна система керування гравіювальним верстатом розроблена під час виконання бакалаврського дипломного проекту.

В ході розробки:

1. Проведено аналіз методів побудови існуючих комп'ютерних систем автоматизації управління виробництвом.
2. Сформульовані вимоги до комп'ютерної системи керування гравіювальним верстатом.
3. Розроблена структурна схема системи керування.
4. Розроблено функціональну схему контролера.
5. Розроблено блок-схему системи керування.
6. Побудований макетний взірець

Модуль керування складається з плати *Arduino Mega* з вбудованим мікроконтролером *ATmega*2560. Для роботи з *Arduino* використано плату *RAMPS* 1.4.

Макет трьохосьового гравіювального верстату складається з фрезерного вузла фірми *Titan* (керування шпинделем виконується в ручному режимі), крокових двигунів *Nema17 (NEMA* 17*HS*4401 та *NEMA* 17*HS*8401*)*, які виконують функції виконавчих механізмів, а давачі використовуються як механічні кінцевики.

7. Розроблена програма керування гравіювальним верстатом, яка відлагоджена макетному взірці.

Висновки

Комп'ютерна система керування гравіювальним верстатом може бути використана для обробки відносно невеликих дерев'яних

поверхонь в домашніх умовах, а також дана система може бути розглянута в навчальних цілях у вищих навчальних закладах або використана як складова частина складніших систем гравіювання.

РОЗРОБКА МОБІЛЬНОГО ДОДАТКУ ANDROID ТА ВСЕУНІВЕРСИТЕТСЬКОЇ БАЗИ ДАНИХ УСПІШНОСТІ СТУДЕНТІВ ДЛЯ АВТОМАТИЗОВАНОГО ОБЧИСЛЕННЯ ЇХ СЕМЕСТРОВОГО РЕЙТИНГУ ТА ВИЗНАЧЕННЯ СТИПЕНДІАТІВ.

Харук С.С.

ДВНЗ „Ужгородський національний університет”
88000, Ужгород, вул. Волошина, 54

В усіх університетах держави, студенти які навчаються на денній формі за свої успіхи у навчанні отримують стипендії. Не завжди процес обчислення їх рейтингу є легким та централізованим. Також, через помилки методистів або людей які займаються обчисленням цього рейтингу, не завжди вірно визначаються стипендіати. Як кінцевий результат – студенти можуть залишитися без стипендії, а процес «апеляції» може займати декілька місяців.

На даний момент в УжНУ використовується наступний механізм обчислення рейтингу та визначення стипендіатів:

- Викладач, прийнявши залік/іспит у студентів, записує дані успішності у відомість;
- Деканат вносить дані успішності по всім студентам факультету у «зведені відомості»;
- «Зведені відомості» передаються до обчислювального центру ДВНЗ «УжНУ», в якому дані успішності студентів безпосередньо вносяться в базу даних;
- Комп’ютерна програма вираховує по заданій формулі загальний рейтинг всіх студентів університету та створює кінцевий список.

Недоліки даного підходу:

- «бюрократичний радянський підхід»;
- велика кількість посередників;

- збільшується ймовірність помилок;
- нецентралізованість;
- втрата часу;

Метою моєї роботи є створення додатку Android за допомогою якого викладач безпосередньо після закінчення заліка/іспита зі свого акаунта вносить дані успішності у всеуніверситетську базу даних, з якої в майбутньому в один клік формується рейтинг та список стипендіатів.

ПРОЕКТУВАННЯ, МОНТАЖ ТА КОНФІГУРУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ IP-ТЕЛЕФОНІЇ КАФЕДРИ ТВЕРДОТІЛЬНОЇ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Кравець Є.В.

ДВНЗ „Ужгородський національний університет”
88000, Ужгород, вул. Волошина, 54

Кожен сучасний заклад чи підприємство використовує телефонну і комп'ютерну мережу. А це означає, що для підтримки працездатності кожної з них потрібні значні витрати. Адже, використання двох мереж комунікацій збільшує обсяги даних, що використовуються у кожній з мереж.

Вирішення цієї проблеми полягає у виборі універсальних комунікацій. Тому що, можливості звичайної телефонної мережі обмежуються здатністю передавати голос і факсимільні повідомлення. В той час, як за допомогою універсальних комунікацій можна створювати відеоконференції, надсилати текстові повідомлення або електронні листи, здійснювати автоматизоване перенаправлення і зберігати інформацію про абонента. І це не всі переваги.

При такому підході корпоративна телефонія, відеоконференції і мережа передачі даних більше не будуть ізольованими системами, кожна з яких вимагає своєї власної інфраструктури і власних засобів управління.

Метою моєї роботи є розробка та монтаж мережі IP-телефонії на кафедрі твердотільної електроніки та інформаційної безпеки. На даний момент проведено аналіз існуючих програмних продуктів для реалізації пакетної телефонії в мережі кафедри. Також була вивчена апаратна частина, що використовується для передачі голосової інформації по локальних мережах. Після чого була розроблена схема впровадження VoIP з використанням вже наявної локальної мережі. Крім того, було проведено аналіз обладнання і програмного забезпечення. В результаті прийнята до впровадження багатофункціональна апаратна частина і надійне серверне програмне забезпечення, а також, вирішені основні проблеми існуючої мережі.

ОСОБЛИВОСТІ КОНФІГУРАЦІЇ БАГАТОСИСТЕМНИХ ПК

Гайсак А.І.
ДВНЗ „Ужгородський національний університет”
88000, Ужгород, вул. Волошина, 54

Всім нам відомо, що левову долю (84,32%) ринку комп’ютерних операційних систем займає продукт компанії Microsoft – Windows. Не залежно від версії системи без сумніву вона є одною з найзручніших, але виникають ситуації коли функціональності Windows не вистачає. До таких ситуацій відноситься програмування для смартфонів на iOS (для цього нам потрібний комп’ютер який має на борту систему MacOS) або проведення деяких обчислень де зручніше використовувати Linux. Якщо у випадку з Linux все більш-менш зрозуміло, то для використання системи MacOS нам потрібно купувати комп’ютери компанії Apple які м’яко кажучи не дешеві та й взагалі є дуже специфічними продуктами які підійдуть не кожному. Тому й виникає питання : «Що робити якщо функціоналу твоєї системи тобі попросту не вистачає?». Ну що ж, робота яку я виконав зможе відповісти на ваше питання. В даній роботі ми будемо встановлювати на ПК аж 3 операційні системи, а саме:

1) MacOS ; 2)Windows; 3)Linux.

Нагадаю, що це все ми будемо робити на звичайнісінькому ноутбуці із системою Windows на борту. Для виконання даної роботи нам потрібно буде всього на всього один флеш накопичувач розміром 8гб. Для початку нам потрібно завантажити першу операційну систему (MacOS). Знайти ми її можемо на будь-якому торрент-трекері або на спеціалізованих форумах тематика яких Макінтош або Хакінтош. Також нам знадобиться «правильний» загрузчик, який би міг якісно справитися з оперуванням цих 3-ьох систем. Одним із таких є Clover Bootloader.

Встановлення MacOS

Спершу за допомогою спеціалізованої програми TransMAC ми розділимо наш флеш-накопичувач на два сектори:

1) Сектор виділений для Clover ;

2) Сектор виділений для установочного образу системи MacOS.

Далі нам потрібно попередньо завантажити усілякі дрібнички які допоможуть нам запустити систему MacOS на нашому ПК. Так як система MacOS створюється тільки під ПК від компанії Apple то запустити її на інших ПК без додаткових дій не вдасться. Спершу нам потрібно дізнатися які комплектуючі встановлені саме в нашому ПК та порівняти їх із комплектуючими які використовуються в ПК від компанії Apple. Коли ми знайшли та склали список комплектуючих які не збігаються з вищевказаними то треба знайти метод як їх зробити працюючими сам під системою MacOS.

Якщо наприклад у системі Windows для цього використовуються драйвери, то у системі від Apple використовуються так звані кексти. Все що нам потрібно, це знайти кексти на наші комплектуючі та скопіювати їх на розділ флешки з Clover. Також до кожного кекста в комплект іде кілька рядів коду. Ці ряди – інструкції для системи про те, як потрібно працювати з тим чи іншим комплектуючим. Ці рядки потрібно внести до спеціального файлу DSDT який також можна знайти на розділі флешки з Clover. Звичайно бувають випадки, що на таких форумах можна знайти готові підготовлені кексти та DSDT файли для вашого ноутбуку, але так як моделей є безліч (навіть із максимально схожими комплектуючими) краще пройти весь цей вищевказаний процес й самому налаштувати загрузчик.

Після виконання всіх цих дій установка системи MacOS повинна запуститись.

Встановлення Windows

Якщо ми хочемо встановити Windows та інші системи MacOS то нам потрібно заздалегідь (під час установки MacOS) розділити наш жорсткий диск на 2 або 3 розділи. На відміну від звичайного встановлення Windows цей процес відрізняється тільки тим, що загрузочний флеш-накопичувач повинен підтримувати UEFI встановлення, а також встановлення повинно відбуватися через загрузчик Clover, а не через BIOS ПК.

Встановлення Linux

У випадку Linux різниці між простим встановленням і встановленням поверх MacOS такі самі як у Windows. Після виконання цих дій при запуску ПК ми отримаємо вікно в якому нам дадуть обрати систему для запуску. Цим самим ми зможемо використовувати всі 3 системи для наших потреб та зручностей.

РОЗВИТОК WEB ТЕХНОЛОГІЙ.

Галас С.С.

ДВНЗ „Ужгородський національний університет”
88000, Ужгород, вул. Волошина, 54

Сучасний стан інформаційні технології - сукупність засобів і методів обробки даних. Інтернет - міжнародне об'єднання комп'ютерних мереж, яке використовує доменну адресацію та IP-протокол. Види інформаційних технологій в залежності від оброблюваної інформації: СУБД, алгоритмічні мови, табличні процесори, текстові процесори, гіпертекст, графічні процесори, експертні системи, засоби мультимедіа. Зараз все йде до інтеграції ... Як правило, все йде в загальному комплекті. Web 1.0 Системи кошиків для покупок, які більшість власників веб-сайтів електронної торгівлі використовує в деякому вигляді або формі, в основному підпадають під категорію.1.0. Загальна мета полягає в поданні продукції для потенційних клієнтів, так само як це робить каталог або брошура, тільки з веб-сайту ви можете також надати спосіб покупки продукції для будь-якого користувача в світі. Інтернет забезпечив вектор для надання, і видалив географічні обмеження.

WEB 0.0 - юзер мріє законектитись з ким або чим небудь;
WEB 1.0 - юзер отримує контент;
WEB 2.0 - юзер створює контент;
WEB 3.0 - колективне створення контенту;
WEB 4.0 - контент думає за юзера;
WEB 5.0 - контент спілкується з контентом;
WEB 6.66 - контент видаляє юзерів, зрозумівши що вони не мають сенсу;
WEB 7.0 - весь контент самовидаляється, зрозумівши що в ньому нема сенсу.

Невеликий (за історичними мірками) термін існування сервісу WWW показав його потребу все зростаючому числу користувачів. Це стало хорошим стимулом для розвитку веб-орієнтованих концепцій і технологій, що збільшують можливості користувачів. Масове впровадження і використання цих рішень - причина якісних змін у Всесвітній павутині, свого роду зміна «версії» Web. На поточний

момент аналітики Інтернет виділяють три таких «версії» - Web 1.0, Web 2.0 та Web 3.0 (варто зазначити, що поділ цей умовний і часто критикований).

Всесвітня павутина (www), або просто Web, існує вже більше двох десятків років. За цей час відбувалися зміни в технологіях подання інформації та взаємодії з користувачем. Можна сказати, що Веб побудований на протоколах, контенті (інформації та даних), серверних і клієнтських скриптах. Можна виділити кілька етапів-ер розвитку Web, що відображають шлях його еволюції. Ці ери не приходять на зміну один одного, а як би накладаються один на одного, привносячи нові можливості і лише частково замінюючи старі технології. Свобода і демократичність мережі, відсутність соціальних стримуючих факторів дозволяє легко проявлятися передовим ідеям. Інтернет дозволяє зацікавленим і здатним людям об'єднуватися, створюючи більш великі проекти. Простежимо основні етапи розвитку технологій Web. 90-і роки XX століття Web-вміст статично, для його структуризації та оформлення використовується мова гіпертекстової розмітки HTML. Однак головне, що дає HTML, полягає в гіпертексті: web являє собою не окремі документи, а взаємопов'язану мережу документів. Самі документи залишаються статичними. Початок XX століття Це ера LAMP+Linux + Apache + Mysql + PHP. Найважливішим компонентом web-технологій стають бази даних, що зберігають вміст сайту. Сторінки динамічно формуються за допомогою мови програмування на сервері в залежності від приходять запитів користувача. Далі на клієнтський комп'ютер відправляється готовий HTML-документ.

Застосування інтернет і Web-технології у навчальній діяльності. Перспективним напрямом розвитку сучасної освіти є, можливість створення комфортних умов, з погляду забезпечення організації навчальної діяльності, за рахунок створення інформаційно-комунікаційної освітньої середовища. Основними складовими цього середовища мають стати досягнення якості освіти, які диктуються обновляющимися стандартами освіти нового покоління і дидактичними можливостями засобів інформаційно-комунікаційних технологій (ІКТ) і Web-технологій. Процес розвитку комп'ютерних технологій, Web-технологій і телекомунікацій неминуче призвів до інформатизації різних видів освітньої діяльності, зокрема створення інформаційно-освітнього простору. Рівень розвитку освіти,

пред'явлення нових вимог до якості освіти світового співтовариства передбачає формування в учнів особистого досвіду присутності в інформаційно-освітньому просторі. Пріоритетними напрямками створення інформаційно-освітнього простору є, впровадження та використання дидактичних можливостей ІКТ, Web-технологій (Web-сервіси, освітні Web-ресурси, мережеві співтовариства) у навчальний процес середньої та вищої освіти.

Технологія пошукової системи.

Google змусив світ пошукових систем перевернутися з ніг на голову завдяки своїй концепції PageRank, яка виявилася справжнім технологічним проривом і яку зараз використовує більшість провідних пошукових систем для забезпечення більш якісного пошуку. «Технологія пошуку PageRank компанії Google працює шляхом, в першу чергу, встановлення структури посилань у всій мережі, а затії ранжуючи кожну окрему сторінку, грунтуючись на числі і значущості посилань на неї на інших сторінках».

Останнім часом, представники компанії Google, дуже часто стали відзначати, що їх пошуковий робот часто починає індексувати дублююче зміст сторінок, а це в певних випадках призводить до значного скорочення кількості проіндексованих сторінок і зниження частоти їх виникнення в індексі пошукової системи. Дублює зміст часто з'являється, в тих ситуаціях, коли на певному сайті, однакова інформація може надаватися за різними URL-адресами, наприклад при використанні ідентифікаторів сеансу яких інших подібних параметрів.

ВИЯВЛЕННЯ ВРАЗЛИВОСТІ 0-DAY У WI-FI АДАПТЕРАХ

Пішковцій М.-О.І.

Державний вищий навчальний заклад «УжНУ»
88000, Ужгород, вул. Волошина, 54

Кожен із нас користується Інтернетом. Для того щоб отримати доступ до мережі потрібно канал розповсюдження. Найчастіше це Wi-Fi. Wi-Fi адаптер – це бездротова мережа, яка підключає сотні користувачів до всесвітньої мережі Інтернет. Потрібно знати лише пароль!

Але програмне забезпечення Wi-Fi адаптера не досконале. Атака нульового дня виникає, коли комп'ютер зловмисника намагається використовувати вразливості в програмному забезпеченні, які невідомі або не закриті виробником. На сьогоднішній день через витонченість та величезну кількість атак нульового дня стає загальноприйнятним, що мережні атаки досягнуть цілі. Успішність захисту тепер вимірюється тим, наскільки швидко мережа зможе відреагувати на атаку. Ідеальна мета - здатність виявляти атаки, які відбуваються в режимі реального часу, а також припиняти їх відразу або протягом кількох хвилин. На жаль, багато компаній та організацій сьогодні не можуть виявити такі атаки впродовж кількох днів чи навіть місяців після їх появи.

Зловмисники часто розгортають підроблені точки доступу Wi-Fi адаптера , щоб заманити користувачів. Оскільки атакуючий має доступ до всієї інформації, переданої через скомпрометовану точку доступу, користувачі, підключені до цієї точки доступу, піддаються ризику. Ніколи не використовуйте невідомі точки Wi-Fi, не шифруючи трафік через VPN. Ніколи не передавайте конфіденційні дані, такі як номери кредитних карток, під час використання невідомої мережі (дротової або бездротової). Щоб забезпечити безпеку і приватність Wi-Fi адаптера потрібно дотримуватись «правил безпеки». Якщо ви хочете зберегти конфіденційність у бездротовій мережі поширюйте якомога менше інформації. Вам не варто ділитись або створювати паролі за такою інформацією, як: дата народження, ім’я, прізвище, поштою, номером телефон. Не повідомляйте пароль, не переходьте на незнайомі сайти, не передавайте паролі ідентифікації по мережі Інтернет!

У науково дослідницькі роботі я розказувала про вразливості бездротового адаптера. Показала на практиці слухачам один із багатьох методів використання 0-day на цих пристроях. А також ознайомила їх як можна захистити себе від такої вразливості.

Список використаної літератури

1. https://en.wikipedia.org/wiki/Zero-day_(computing)

Визначення використаних термінів у науковій роботі.

2. http://github.com/sophron/wifiphisher.git

Програмний код, який був використаний.

3. https://www.kali.org/downloads/

Сайт із завантажувальною ОС «Kali Linux 2.0»

РОЗРОБКА СИСТЕМИ ПЛАНУВАННЯ РЕСУРСІВ (ERP-СИСТЕМА) ДЛЯ АВТОМАТИЗАЦІЇ ОБЛІКУ УСПІШНОСТІ СТУДЕНТІВ

Фучко К. П.
Державний вищий навчальний заклад «УжНУ»
88000, Ужгород, вул. Волошина, 54

На даний момент, при переході від паперового документообігу до електронного, постає завдання в створенні єдиної системи, яка б дозволяла вести облік всіх процесів. Після аналізу українського ринку було вирішено створити систему планування ресурсів (ERP-систему), яка призначена для автоматизації обліку й управління. Системи саме такого плану дозволяють охопити необхідні відділення (кафедри) фізичного факультету і згрупувати їх в одній системі для зручного ведення обліку успішності студентів.

Під час дослідження сучасних мов програмування, для розроблення даної системи, було обрано мову JavaScript для побудови серверної частини та Angular2 для інтерфейсу. Було проаналізовано наявну систему обліку успішності студентів, та на її основі створене програмне забезпечення, щоб автоматизувати цей процес. Веб-додаток містить розділи для студентів, викладачів та адміністрації (деканату), кожен з яких має свій функціонал та рівні доступу до інформації.

Впровадження ERP-системи значно спрощує облік успішності студентів та процес обміну необхідної інформації між суб’єктами навчального процесу на прикладі фізичного факультету ДВНЗ “Ужгородський національний університет”.

РОЗРОБКА ЗАХИЩЕНОГО БАГАТОФУНКЦІОНАЛЬНОГО СХОВИЩА ПЕРСОНАЛЬНИХ ДАНИХ ДЛЯ ANDROID

Шиченко В. В.
Державний вищий навчальний заклад «УжНУ»
88000, Ужгород, вул. Волошина, 54

Перший етап розробки полягав у встановленні засобів для роботи з Android в Unity. Зокрема, Android SDK потрібної платформи і включення пристрою в систему. Також, необхідне було встановлення Java Development Kit. Використання даного пакету необхідно для виконання базових операцій з пакування .apk пакета і розширення функціональності за допомогою Java-плагінів. Для створення Java - плагінів необхідно було також завантажити Eclipse IDE.

Другий етап пролягав в уточненні деталей технічного завдання, а саме в розробці концепції меню додатка. Схеми основних робочих вікон були розроблені виходячи з ергономічного та інтуітивно зрозумілого вигляду меню.

На третьому етапі, відбувалась безпосередньо реалізація додатку. Для створення візуальної части додатка використовувались елементи GUI .

Збереження інформації було реалізоване в папці додатку, у виді файлу із зашифрованим змістом.

Для виводу нагадування від додатку був написаний окремий плагін в IDE Eclipse на мові Java.

У Unity робота з додатком була організована шляхом використання посилання на додаток, який був підключений у виді бібліотеки AndroidNotifications.

Для шифрування информації реалізований метод шифрування Віженера. Вибір даного методу був обумовлений можливістю використання диференційованих паролів для різних записів. Водночас, залишилась можливість використання «універсального» паролю.

ФОТОІНДУКОВАНІ ЗМІНИ МІКРО-І НАНОТВЕРДОСТІ ВИКОРИСТОВУВАНИХ У ГОЛОГРАФІЧНОМУ ЗАХИСТІ ІНФОРМАЦІЇ ПЛІВОК СИСТЕМИ GE-AS-SE

Планчак О.І.

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Університетська, 14

В наш час швидкими темпами розвиваються інформаційні технології, вони проникають в усі сфери людської діяльності, тому дуже гостро постає питання інформаційної безпеки. З кожним днем технології обробки інформації удосконалюються, а разом з цим підвищуються вимоги до практичних методів забезпечення безпеки. Звичайно, не існує універсальних методів для забезпечення безпеки, адже кожна комп'ютерна система має свої особливості. У наші дні інформація є одним із найцінніших і найкоштовніших ресурсів. Оскільки людство дуже швидкими кроками відходить від зберігання паперових, а все більше і більше віддається перевага електронним носіям, які можуть зберігати інформацію десятиліттями. Також із входом у наше життя комп'ютерів життя суттєво полегшало, тепер десь у замкненій кімнаті стоїть сервер на якому зберігається вся інформація і не потрібно нікуди ходити, нічого носити переписувати, усе робиться за допомогою кількох кліків мишкою, або набором кількох команд.

Одним з перспективних матеріалів для запису оптичної інформації, є плівки халькогенідних склоподібних напівпровідників. Ці матеріали цікаві тим, що для зчитування інформації не вимагається процес прояву та інформація може зчитуватися одночасно з процесом запису, тобто в реальному часі. Іншими перевагами таких матеріалів є:

1. Можливість фазового запису інформації, що обумовлює відсутність амплітудних втрат при зчитуванні інформації або відновлення хвильових фронтів дифракційних елементів.

2. В результаті фотоструктурних трансформацій у плівках спостерігаються рекордно великі зміни показника заломлення, що дозволяє в тонких шарах отримувати фазові затримки в кілька довжин хвиль.

3. Висока оптична однорідність плівок по товщині при напиленні у вакуумі на великі поверхні.

Розглянемо процес створення голограми - голографічного зображення якого-небудь об’єкта. У звичайній чорно-білій фотографії на фотоносію фіксується тільки інтенсивність світла, відображеного об'єктом, і відсутні відомості про фазу світлового променя, що приходить на носій. На відміну від звичайної фотографії на голограмі записується інтерференційна картина, утворена накладанням опорного світлового променя і променя, відбитого від об'єкта. При цьому на голограмі фіксується інформація про амплітуду і фазу світлових хвиль, відбитих від об'єкта.

Голографічні захисні елементи:

- виготовляють у формі знаків (етикеток, наклейок тощо), габаритні розміри та форма яких встановлюються замовником і визначаються призначенням та умовами експлуатації об'єкта захисту;
- як правило, мають багатошарову структуру, яка містить крім носія зображення шари іншого функціонального призначення (захисний, клейовий тощо). Зокрема, з метою підвищення експлуатаційної стійкості поверхня носія зображення вкривається прозорим захисним шаром, спроба відділення якого від голографічного захисного елемента повинна призводити до невиправного пошкодження (руйнування);
- наносяться на об'єкт захисту способом, що забезпечує зберігання його під час експлуатації цього об'єкта та руйнування голографічного захисного елемента в разі вчинення спроби відділення від об'єкта. Безпосереднім носієм зображення може бути фольга гарячого тиснення, інший носій чи сам об'єкт захисту (наприклад, упаковка лікарського засобу). На носій може наноситися зображення реального об'єкта, макета, малюнка, транспаранта, товарного знака або інших стилізованих об'єктів, у тому числі й синтезованих за допомогою комп'ютерної графіки.

З метою ускладнення підробки в зображення голографічного захисного елемента вводять спеціальні елементи, позначки, знаки або символи, у тому числі приховані чи закодовані. Для цього використовують оптичні ефекти, що змінюють вид, масштаб чи

кольорові гами зображення при зміні умов чи способу їх освітлення або спостереження, та елементи, виготовлені з використанням інших технологічних прийомів.

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Наливайко В.И. Получение фазовых структур в оптических материалах / В.И. Наливайко, Г.С. Юрьев, Б.Г. Гольденберг, М.А. Пономарева // "Поверхность". Рентгеновские, синхротронные и нейтронные исследования. – 2003. – № 11. – С. 52–55.

2. Різак В.М. Функціональні халькогенідні напівпровідники / В.М. Різак, І.М. Різак, Д.Г. Семак. — Ужгород: Закарпаття, 2001.— 152 с.

3. Способ записи информации на халькогенидной пленке // Режим доступу: http://www.freepatent.ru/patents/2298839

4. Nalivaiko V.I., Yuryev G.S. Structural Studies of As2S3 Chalcogenide Films by X-Ray Synchrotron Radiation. Proc. of X APAM Topical Seminar and III Conference "Materials of Siberia" – "Nanoscience and Technology", 2 – 6 June, 2003, Novosibirsk, Russia, Nikolaev Institute of Inorganic Chemistry SB RAS, Novosibirsk, 2003. P. 422–423.

5, Генуарио Леа. «Умные» этикетки [Електронний ресурс]. — Режим доступу: http://www.publish.ru/fsp/2008/06/5609038/.

РОЗРОБКА ЦЕНТРАЛІЗОВАНОГО ЗАСОБУ ДИСТАНЦІЙНОГО НАВЧАННЯ ДЛЯ ВИЩОЇ ОСВІТИ

Деяк С.С.

ДВНЗ «Ужгородський національний університет»
88000, Ужгород вул. Волошина, 54

В Україні та багатьох інших країнах, дистанційні форми навчання до недавнього часу не застосовувалися в широкому масштабі через низку об'єктивних причин – в основному через недостатній розвиток та не досить широке розповсюдження технічних засобів нових інформаційних та телекомунікаційних технологій.

В даний час у нашій країні вже створені технічні передумови для широкого використання дистанційного навчання в освіті. Більш того, намітилося відставання реалізації ідей ДО від можливостей, що надаються технічними засобами. Значна кількість українських вищих навчальних закладах (ВНЗ) вже мають діючі кафедри, а й подекуди навіть й інститути, з дистанційного навчання в своєму складі. Саме тому **актуальною є** потреба створити інформаційно-комунікаційне забезпечення для підтримки дистанційного навчання в Ужгородському Національному університеті.

Метою роботи є дослідження генезису дистанційного навчання в широкій історичній, географічній і соціально-педагогічній ретроспективі, виявлення внутрішніх взаємозв’язків сучасних поглядів на дистанційне навчання з їхніми історико-педагогічними аналогами, огляд провідних публікацій з проблем дистанційного навчання за останнє десятиліття. А також розробка програмного засобу для підтримки дистанційного вивчення курсу «Програмування».

Для досягнення поставленої мети необхідно виконати такі **завдання:**

1) Розглянути особливості дистанційного навчання, його генезис.
2) Дослідити розвиток дистанційної освіти в Україні та закордоном.
3) Вивести використання даного виду навчання на новий рівень.
4) Виявити можливості та переваги додатку Google Sites в порівняні з іншими системами.
5) Створити сайт для дистанційного вивчення курсу «Програмування».

Об'єктом дослідження є процес створення інформаційно-комунікаційного забезпчення для підтримки дистанційного навчання

Предметом дослідження є технологія створення інформаційно-комунікаційного забезпечення для підтримки дистанційного навчання

Практичне значення отриманих результатів: Розроблений програмний засіб може використовуватись для вивчення курсу «Програмування» як з власної потреби та ініціативи так і як додаток для вивчення курсу в університеті.

Даний сайт призначений для вивчення курсу «Програмування» за навчальною програмою УжНУ.

Він може використовуватись як для самостійного вивчення предмету, так і як допоміжний матеріал при вивченні «Програмування» в університеті.

Тут ви зможете знайти:

- навчальний матеріал
- завдання до лабораторних робіт з контрольними питаннями
- приклади виконання завдань
- тест-контроль
- корисні лінки

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Абакумова О. О. Дистанційна освіта: суть, основні характеристики, перспективи розвитку / О. О. Абакумова // Держава і глобальні соціальні зміни: історія, теорія, ідеологія: матеріали Міжнар. наук.практ. конф. соціол. 2829 жовтня 2010 р. / Уклад.: Б. В. Новіков, Л. М. Димитрова, П.В.Кутуєв. – К.: НТУУ "КПІ", 2010. – С. 123124.

2. Адаменко О. В. Використання нових інформаційних технологій – необхідна умова входження вишів України в світовий освітній простір / О. В. Адаменко // Освіта Донбасу. – 2007. – № 5 – 6. – С. 5 – 9.

3. Андреев А. А. Дидактические основы дистанционного обучения / А. А. Андреев. — М. : Издательство МЭСИ, 1997. — 248 с

4. Андреев А. А., Солдаткин В. И. Дистанционное обучение: сущность, технология, организация / А. А. Андреев, В. И. Солдаткин. – М.: МЭСИ, 1999. – 196 с.

5. Андреев А.А. Дидактические основы дистанционного обучения в высших учебных заведениях.// М., 1999. – 289 С.

6. Бурік М. Стан та тенденції розвитку системи освіти України в умовах глобалізації / М. Бурік. – К.: Четверта хвиля, 2007. – 48 с.

7. Кухаренко В.М., Рибалко О.В., Сиротенко Н.Г. Дистанційне навчання: Умови застосування. Дистанційний курс: Навч. пос. 3-є вид. / За ред. В. М. Кухаренка. Харків, 2002.- 320 С.

8. Наталія Жевакіна З ІСТОРІЇ ДИСТАНЦІЙНОЇ ОСВІТИ // ВІСНИК ЛЬВІВ. УН-ТУ Серія педагогічна. 2003. Вип.17. С. 135-141

9. Семеріков С. О. Мобільне навчання: історія, теорія, методика / С. Семеріков, І. Теплицький, С. Шокалюк // Інформатика та інформаційні технології в навчальних закладах. – 2008. – №6. – С. 72–82 ; 2009. – №1. – С. 96–104.

10. Семеріков С. О. Мобільне програмне забезпечення навчання інформатичних дисциплін у вищій школі / Семеріков С. О., Мінтій І. С., Словак К. І., Теплицький І. О., Теплицький О. І. // Науковий часопис Національного педагогічного університету імені М.П. Драгоманова. Серія №2. Комп’ютерно-орієнтовані системи навчання : зб. наукових праць / Редрада. – К. : НПУ імені М. П. Драгоманова, 2010. – №8 (15). – С. 18–28.

11. Семеріков С. О. Фундаменталізація навчання інформатичних дисциплін у вищій школі : [монографія] / Сергій Олексійович

12. Семеріков; науковий редактор академік АПН України, д. пед. н., проф. М. І. Жалдак. - Кривий Ріг: Мінерал; К.: НПУ ім. М. П. Драгоманова, 2009. - 340 с.

13. Смирнова-Трибульская Е. Н. Основы формирования информатических компетентностей учителей в области дистанционного обучения: [монография] / Евгения Николаевна Смирнова-Трибульская; научный редактор: академик АПН Украины, д. пед. наук,проф. М. И. Жалдак. - Херсон: Айлант, 2007. - 704 с.

14. Турик Л. А. Педагогические технологии в теории и практике : учеб. пособие / Турик Л. А. — М.: Феникс, 2009.

15. Хуторской А. В. Дистанционное обучение и его технологии // Компьютерра. — 2002. — № 36. — С. 26-30.

СТВОРЕННЯ АНТИВІРУСНОЇ ПРОГРАМИ (ANTVUZH)

Кейс В.С.

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Університетська, 14

Безпека в сфері інформаційних технологій - це комплекс мір, і вона повинна сприйматися як система. Комп'ютерна безпека має різні аспекти, серед яких не можна виділити більш значимі або менш. Тут важливо все. Не можна відмовитися від якоїсь частини цих мір, інакше система не буде працювати.

Саме тому на даний момент часу є актуальним питання захисту інформації кожного користувача. В даній роботі відображено частково вирішенням питання безпеки завдяки створенню програмного продукту - антивірус.

Даний продукт надає можливість:

- **Сканування файлів і програм в режимі реального часу;**
- **Сканування комп'ютера на вимогу;**
- **Відновлення пошкоджених файлів (лікування, поки не передбачено, але в етапі розробки).**

Для реалізації описаних функцій мобільний пристрій забезпечує наступні технічні вимоги:

– операційна система: *Windows 7* і вище;

Розроблений програмний продукт характеризується економним і надійним використанням ресурсів.

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Шорошев В. В. та інші. Класифікація комп'ютерних вірусів і основи захисту від них. Журнал “Бизнес и безопасность” № 2, 2010 р.
2. Шорошев В. В. Основи формування політики безпеки комп’ютерних систем. Наукове видання. Бизнес и безопасность, К., 2006. – с.141.
3. А. Ю. Ільніцький, В. В. Шорошев, І. Л. Близнюк. Монографія “Базова модель експертної системи оцінки безпеки інформації в комп‘ютерних системах органів внутрішніх справ України”

(шифр “Торсіон-1”). Свідоцтво Державного департаменту інтелектуальної власності Міносвіти і науки України про реєстрацію авторського права на твір № 14446 від 20.

4. http: / / www. viruslist. com

РОЗРОБКА САЙТУ КАФЕДРИ ТВЕРДОТІЛЬНОЇ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УЖНУ І СИСТЕМИ ЙОГО ЗАХИСТУ

Рокосовик В. О.
ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54

Веб-сайт є засобом підтримки і розвитку будь-якого підприємства, особливо університету в цілому і його кафедр. Розробка сучасного сайту для кафедри твердотільної електороніки та інформаційної безпеки УжНУ сприяє якісному інформуванню студентів та викладацького складу. Завдяки вичерпній інформативності сайту абітурієнти можуть з легкістю обрати спеціальність та дізнатись про всі події з життя кафедри.

Даний сайт створено на основі мови програмування JavaScript, оскільки саме ця мова повністю задовольняє потреби в даній задачі. Для зручного і захищеного адміністрування використовується база даних MySQL. Також даний сайт має сучасний інтерфейс, для використання якого було використано Angular.

В даній роботі розроблено Веб-сайт, який використовує SHA-256 для зберігання паролів, що забезпечує надійність сайту і розмежування доступу між користувачами і адміністратором.

Загальні характеристики нового веб-сайту:

- швидкість роботи; захист від веб-атак;
- зручний інтерфейс;
- можливість управління інформаційним вмістом сайту.

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. JavaScript. URL: https://ru.wikipedia.org/wiki/JavaScript
2. Node.js: URL: https://uk.wikipedia.org/wiki/Node.js
3. Paul DuBois. MySQL Cookbook, - August 1997, August 2014, O'REILLY.
4. Matt Frisbie. Angular 2 Cookbook, - 2017, Packt Publishing.
5. SASS: URL: https://en.wikipedia.org/wiki/Sass_(stylesheet_language)
6. Nathan Rozentals. Mastering TypeScript, - 2017, Packt Publishing
7. R. N. Taylor, N. Medvidović and E. M. Dashofy, Software architecture: Foundations, Theory and Practice. Wiley, 2009.

ПРОБЛЕМИ ЗАХИСТУ СОЦІАЛЬНИХ МЕРЕЖ

Чопей Є.В

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54

В останні два десятиліття інформаційні технології здійснили справжній прорив. І в результаті утворились задачі які потрібно вирішувати інформаційній безпеці і в даній сфері. Достатньо багато інформації зловмисник про свою потенційну жертву може знайти у відкритих джерелах, наприклад в соціальних мережах. Взагалі, соціальні мережі - це велике зло. Люди своїми руками пишуть досьє на самих себе та викладають це всім на огляд.

З технічної сторони захисту інформації в соціальній мережі, зловмисник може нанести шкоди як клієнту (користувачу) та і розробникам. Якщо ж зловмиснику це вдалось, то зрозуміло, що частіше за все це вина розробників. SSL (рівень захищених сокетів) — криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і сервером. SSL спочатку розроблений компанією Netscape Communications . Згодом на підставі протоколу SSL 3.0 був розроблений і прийнятий стандарт RFC, що отримав ім'я TLS. До того як був запроваджений даний протокол, могла бути здійснена атака MitM (Man-in-the-Middle). Де зловмисник представлявся для клієнта - сервером, а для сервера клієнтом тим самим перехоплював повідомлення з обох сторін.

Атака буде успішною, якщо:

- Сервер не має підписаного сертифіката;
- Клієнт не перевіряє сертифікат сервера;
- Користувач ігнорує повідомлення про відсутність підпису сертифіката центром сертифікації або про розбіжності сертифіката з кешованою копією.

Якщо зловмисник зможе підмінити сертифікат SSL на свій то він зможе розширувати всі вхідні і вихідні повідомлення клієнта. А це загрожує не тільки розкриттю конфіденційних даних клієнта, але й серверу, якщо клієнт мав достатньо широкий рівень доступу. Тим самим зловмисник зможе скопіювати потрібну йому інформацію з серверу або навіть видалити всю базу даних.

Дану проблему я вирішив додатковим RSA з відкритим ключем шифруванням даних для передачі. Навіть якщо у сертифікат зловмисника буде верифіковано як справжній, додаткове шифрування не дозволить йому розпізнати потрібну йому інформацію. А за час, який буде витрачено на дешифрування зловмисником даної інформації, вона вже втратить свою актуальність.

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Информационная безопасность. Защита и нападение - Андрей Бирюков 2017 - 434 с.
2. Нормативная база и стандарты в области информационной безопасности - Ю. Родичев (2017)
3. Е. Баранова, А. Бабаш «Информационная безопасность и защита информации» 3-е изд. (2016)
4. В. Бондарев «Введение в информационную безопасность автоматизированных систем» (2016)
5. С. Нестеров «Основы информационной безопасности» (2016)
6. Ghost in the Wires: My Adventures as the World's Most Wanted Hacker - Kevin Mitnick
7. Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground - Kevin Poulsen

ПОБУДОВА СИСТЕМИ ЗАХИСТУ ПРИМІЩЕННЯ ДЕКАНАТУ ВІД ВИТОКУ ІНФОРМАЦІЇ

Баркоці В. В.

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54

Система захисту інформації має безпосередній вплив на діяльність підприємств. Головна проблема забезпечення захисту інформації полягає в тому, що існує безліч каналів витоку та каналів для несанкціонованого доступу, тому задача забезпечення інформаційної безпеки потребує комплексного підходу. Отже, проблема побудови системи захисту приміщення на об'єкті інформаційної діяльності є актуальною темою для дослідження.

Метою даної роботи є побудова системи захисту приміщення деканату від витоку та несанкціонованого доступу до інформації.

Для планування та розробки системи захисту інформації на об'єкті інформаційної діяльності необхідно побудувати модель загроз, детально розглянути існуючі канали витоку та несанкціонованого доступу, розробити систему захисту, яка буде забезпечувати блокування технічних каналів витоку інформації. Головними технічними каналами витоку інформації є акустичний, віброакустичний, акустоелектричний, оптико - електронний (лазерний), та параметричний канали. Для запобіганню витоку інформації акустичним каналом для прикладу можна використовувати генератори шуму; віброакустичного – використання звукопоглинаючих матеріалів та вібраційних розв'язок; лазерного – використання захищених вікон і т.д.

Але потрібно усвідомити, що ніякі апаратні, програмні, технічні і будь-які інші рішення не зможуть гарантувати абсолютну надійність і безпеку даних. У той же час можна суттєво зменшити ризик втрат при комплексному підході до питань безпеки. Засоби захисту інформації не можна проектувати, купувати чи встановлювати до тих пір, поки фахівцями не проведений відповідний аналіз.

БЕЗПЕЧНІ КОМУНІКАЦІЇ ЧЕРЕЗ ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ (VPN)

Русінко Р.Ю.
ДВНЗ «Ужгородський національний університет»
88000, Ужгород вул. Волошина, 54

Останнім часом у світі телекомунікацій спостерігається підвищений інтерес до віртуальних приватних мереж (Virtual Private Network - VPN). Це обумовлено необхідністю зниження витрат на утримання корпоративних мереж за рахунок більш дешевого підключення віддалених офісів та віддалених користувачів через мережу Internet. Однак необхідно відзначити, що при об'єднанні мереж через Internet, відразу ж виникає питання про безпеку передачі даних, тому виникла необхідність створення механізмів, які дозволяють забезпечити конфіденційність і цілісність інформації, що передається. Мережі, побудовані на базі таких механізмів, і отримали назву VPN.

Метою роботи є побудова та налаштування VPN мережі на основі протоколу IPsec в потужній програмі для моделювання мереж, яка дозволяє студентам експериментувати з поведінкою мереж і оцінювати можливі сценарії розвитку подій, Cisco Packet Tracer. **Об’єктом дослідження є** процес створення віртуальної приватної мережі в середовищі програми Cisco Packer Tracer. **Предметом дослідження є** технологія створення віртуальної приватної мережі в середовищі програми Cisco Packer Tracer.

Практичне значення отриманих результатів: Побудована VPN мережа, яка об’єднує декілька мереж в єдину віртуальну мережу та забезпечує конфіденційність і цілісність переданої інформації. Використання технології VPN доцільно для захисту корпоративної мережі від дії вірусів, зловмисників, а також від інших загроз, які є результатом помилок в конфігурації або адмініструванні мережі.

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А.Олифер. // Учебник для вузов. – 5-е изд. – СПб.: Питер, 2016. – 992с.: ил.

2. Одом, Уэнделл. Официальное руководство по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 / Уэнделл Одом. – 2-е изд.: Пер. с англ. – М.: ООО “И. Д. Вильямс”, 2010. – 672 с. – ISBN 978-5-8459-1439-2.
3. Одом, Уэнделл. Официальное руководство по подготовке к сертификационным экзаменам CCNA ICND2 / Уэнделл Одом. – 2-е изд.: Пер. с англ. – М.: ООО “И. Д. Вильямс”, 2012. – 736 с. – ISBN 978-5-8459-1442-2.
4. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д.Уэзеролл. – 5-е изд. – СПб.: Питер, 2012. – 960 с.
5. Палмер М. Проектирование и внедрение компьютерных сетей / М.Палмер, Р. Синклер. – СПб.: БХВ-Петербург, 2004. – 752с.
6. Нортроп Т. Проектирование сетевой инфраструктуры Windows Server 2008. Учебный курс Microsoft / Т. Нортроп, Дж.К. Макин // Пер. с англ. – М.: Издательство «Русская Редакция», 2009. – 592с. : ил.
7. Моримото Р. Microsoft Windows Server 2008 R2. Полное рук-во / Моримото Р., Ноэл М., Драуби О., Мистри Р., Амарис К. // Пер. с англ. – М.: ООО "И.Д. Вильямс", 2011. – 1456с. : ил.
8. Колисниченко Д.Н. Беспроводная сеть дома и в офисе / Д.Н. Колисниченко. — СПб.: БХВ-Петербург, 2009. — 480с.; ил.
9. Браун Стівен. Віртуальні приватні мережі./ Стівен Браун – М.: Радио и связь, 2001 – 376 с.
10. Владимиров А.А. WI-FI Боевые приемы взлома и защиты беспроводных сетей /А.А. Владимиров, К.В. Гавриленхо, А.А. Михайловский – М.: NT-Press, 2005 – С. 338-347.
11. Медведев Н. Г. Аспекти інформаційної системи віртуальних приватних мереж / Н. Г. Медведев, Д.В. Москалик – К.: Европ. ун–та 2002 – 96 с.
12. Лукацький А. Невідома VPN / Комп'ютер Пресс.-М.: № 10, 2001;
13. Норманн Р. Вибираємо протокол VPN / Windows IT Pro. - М.: № 7, 200;
14. Петренко С. Захищена віртуальна приватна мережа: сучасний погляд на захист конфіденційних даних / Світ Internet. - М.: № 2, 2001;
15. Салліван К. Прогрес технології VPN. PCWEEK / RE, - М.: № 2, 1999.

ПРОГРАМНІ ЗАСОБИ БЕЗПЕКИ ЛОКАЛЬНИХ МЕРЕЖ В ОПЕРАЦІЙНІЙ СИСТЕМІ FREEBSD

Бабич М.О.

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Університетська, 14

Персональний комп'ютер став невід'ємною частиною будь-якого роду людської діяльності. Практично у всіх сферах, починаючи від виробництва і до побуту, від банківської діяльності і до розваг задіяних комп'ютерній техніці. Вони відкрили якісно новий етап в житті і розвитку людської цивілізації.

Проте інформацію, яка міститься на одному комп'ютері, досить важко, особливо при великих об'ємах інформації, перенести на інший, для подальшої роботи. Також коли на кожному пристрої є свої версії документів, важко організувати спільну роботу над ними та синхронізацію. Ці труднощі значно знижують продуктивність праці, але вони майже повністю відпадають з появою комп'ютерних мереж. Комп'ютерні мережі відкрили зовсім нові і значно ширші можливості використання ПК. Тепер ПК – це не тільки засоби для обробки інформації, це – також засоби для отримання та обміну інформацією.

Метою роботи є дослідження засобів безпеки локальних мереж в операційній системі FreeBSD. Може здатись безглуздим розмова про операційній системі FreeBSD з огляду на таких серйозних конкурентів як Mac OS X і Windows. Але в області обчислювальної техніки часто зустрічаються приклади простеньких операційних систем. Чому ж так виходить? Справа в тому, що є такі області обчислювальної техніки в яких застосування таких «титанічних» систем як Windows і Mac OS було б просто не вигідно як в технічному так і в матеріальному плані. Тому і створюються такі системи як FreeBSD.

Разом з цим FreeBSD є операційною системою з відкритим програмним кодом, тобто операційну систему можна модернізувати і навіть в деяких випадках змінювати в корені (крім основного ядра системи). FreeBSD також є системою безкоштовного розповсюдження, тобто ви можете її встановити, чи не виплачуючи грошей за ліцензію. варто також підкреслити, що FreeBSD є UNIX-подібної операційної системою (Тобто похідною від UNIX).

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Майкл Лукас. FREEBSD. Докладне керівництво = Absolute BSD. The Ultimate Guide to FREEBSD. — Спб. : Символ-Плюс, 2004. — 616 с.

2. Babak Farrokhi, Network Administration with FREEBSD 7: Building, securing, and maintaining networks with the FREEBSD operating system, Packt Publishing, April 14 2008, 280 стор.

АВТОРСЬКИЙ ПОКАЖЧИК