КАФЕДРА ТВЕРДОТІЛЬНОЇ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДВНЗ „УжНУ”

УКРАЇНСЬКЕ ФІЗИЧНЕ ТОВАРИСТВО

АКАДЕМІЯ ТЕХНОЛОГІЧНИХ НАУК УКРАЇНИ

7 листопада 2019

УЖГОРОД

V НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

"ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ЖИТТІ СТУДЕНТІВ ТА МОЛОДИХ НАУКОВЦІВ ЗАКАРПАТТЯ"

7 листопада 2019 року

ПРОГРАМА КОНФЕРЕНЦІЇ

Місце проведення: *Велика фізична аудиторія (181),*
фізичний факультет УжНУ,
вул. Волошина, 54, м. Ужгород

УЖГОРОД - 2019

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Морозов А.О. – Почесний Голова, д.тех.н., професор, Заслужений діяч науки і техніки України, академік НАН України, академік Міжнародної Академії інформатики, Президент Академії технологічних наук України;
Смоланка В.І. – Голова, доктор мед. наук, професор, ректор УжНУ, Президент Української асоціації нейрохірургів;
Різак В.М. – заступник голови, доктор фіз-мат. наук, професор, завідувач кафедри ТЕІБ, Заслужений діяч науки і техніки України, Голова ЗВ УФТ, академік та керівник Закарпатського осередку АТН України;
Студеняк І.П. – доктор фіз-мат. наук, професор, проректор з наукової роботи 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 ;
Рубіш В. М. – д. фіз-мат. наук, професор, завідувач Ужгородської лабораторії матеріалів оптоелектроніки та фотоніки Інституту проблем реєстрації інформації НАН України, член-кореспонде́нт Академії технологічних наук України;
Повідайчик М. М. – к. ек. н., декан математичного факультету УжНУ;
Повхан І. Ф. – к. техн. н., декан факультету інформаційних технологій УжНУ;
Туряниця І. І. – к. фіз-мат. н., декан інженерно-технічного факультету УжНУ;
Пагіря М. М. – доктор фіз-мат. наук, професор Мукачівського державного університету;
Біланич В. С. – к. фіз-мат. н., доцент УжНУ, член-кореспонде́нт Академії технологічних наук України;
Попович Н. І. – к. фіз-мат. н., доцент УжНУ;
Мисло Ю. М. – викладач УжНУ;
Барта А. А. – викладач 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;
Смоланка В. І. – Голова, доктор мед. н., професор, ректор УжНУ, Президент Української асоціації нейрохірургів;
Різак В. М. – заступник голови, доктор фіз-мат. наук, професор, завідувач кафедри ТЕІБ, Заслужений діяч науки і техніки України, Голова ЗВ УФТ, академік та керівник Закарпатського осередку АТН України;
Рубіш В. М. – д. фіз-мат. наук, професор, завідувач Ужгородської лабораторії матеріалів оптоелектроніки та фотоніки Інституту проблем реєстрації інформації НАН України, член-кор. Академії технологічних наук України;
Пагіря М. М. – доктор фіз-мат. наук, професор Мукачівського державного університету;
Млавець Ю. Ю. – к.ф.-м.н., заступник декана з наукової роботи математичного факультету УжНУ;
Кут В. І. – к.техн.н., доцент УжНУ;

Сватюк О. Я.- старший викладач УжНУ;
Біланич В. С. – к. фіз-мат. н., доцент УжНУ, член-кореспонде́нт Академії технологічних наук України;
Попович Н. І. – к. фіз-мат. н., доцент УжНУ;
Чобаль О. І. – к. фіз-мат. н., доцент УжНУ;
Барта А. А. – викладач УжНУ;
Маркевич П. В. – викладач УжНУ;
Мисло Ю. М. – викладач УжНУ;
Пірогов О. О. – аспірантУжНУ;
Буковецький В. – аспірантУжНУ
Нейдел Є. – студент УжНУ;
Малицький Б. – студент УжНУ;
Черепов О. – студент УжНУ.

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

Секретар: ***Пішковці Марія-Ольга Іванівна.*** .

09:00	Відкриття конференції - **Різак В. М.,** д. ф.-м. н., професор, завідувач кафедри твердотільної електроніки та інформаційної безпеки УжНУ. Вітальне слово **Смоланки В. І.** - д. мед. н., професора, ректора УжНУ, **Студеняка І. П.** - д. фіз-мат. н., професора, проректора з наукової роботи УжНУ, **Бабинця Ю. Ю. –** головного спеціаліста департаменту освіти і науки Закарпатської ОДА.
09:30	Густі Владислав Володимирович. Використання WiFi Jammer для атак на мережі WiFi та способи захисту
09:45	Буковецький Василь Іванович. Веб-скрапінг: автоматизований збір інформації з Web-ресурсів.
10:00	Черепов Олександр. Розробка ПЗ для перевірки стану сайту.
10:15	Біланич Василь Віталійович. Дослідження процесів релаксації у фоточутливих некристалічних напівпровідниках методом диференціальної скануючої калориметрії.
10:30	Бібен Іван Едуардович. Створення програмного комплексу шифрування інформації в оптоволоконних каналах зв'язку методом RSA.
10:45	Петечук Владислав Васильович, Петечук Ярослав Васильович. Пристрій для розпізнавання та озвучення текстової інформації на базі мікрокомп’ютера Raspberry PI 3
11:00	Гайсак Андрій Іванович. Web-орієнтований інтерфейс віддаленого доступу до віртуальної навчальної лабораторії.
11:15	Гайдук Богдан Анатолійович. Розробка додатків захисту персональних даних з використанням нейронних мереж в ОС Android на мові програмування Java.
11:30	Кава брейк.
12:00	Пекар Руслан Олександрович. Інновації у навчанні.
12:15	Фролов Артем Олександрович. Шифрування кольорових зображень з використанням матриць Адамара.
12:30	Шкомар Юрій Андрійович. Розробка програмного забезпечення верифікації вторинної авторизації.
12:45	Пішковцій Марія-Ольга Іванівна. Заглушувач на базі плати Arduino Nano для захисту мовної інформації.
13:00	Гутич Іван Іванович. Комп'ютерна візуалізація, як засіб подання навчального матеріалу.
13:15	Пирогов Олексій Олександрович. Аналіз автоматичних сканерів уразливостей веб-додатків та мереж.
13:30-	Гелетей Йосип Йосипович. Додаток для виявлення та знешкодження

	шпигунського програмного забезпечення у персональних компютерах.
13:45-	Грабовчак Ярослав Павлович. Додаток для побудови структурної моделі обличчя за допомогою згорткових нейронних мереж.
14:00	Біланич Богдан Віталійович. Елементи технічного захисту інформації на халькогенідних плівках системи As-Se.
14:15	Сосна Андрій Борисович. Мінімізація ризиків інформаційної безпеки філіалу банку "Перший Український Міжнародний Банк" на основі комплексної системи захисту інформації.
14:30	Савенко Євген Васильович. Розробка сайту кафедри твердотільної електроніки та інформаційної безпеки та його захист від Ddos-атак.
14:45	Сивуля Вадим Миколайович. Основні принципи та практична реалізація комплексного захисту інформації на підприємстві "Октава-Фінанс".
15:00	Штец Володимир Юрійович. Квантово-хімічне моделювання поверхні TiO_2 у середовищі QUANTUM ESPRESSO.
15:15	Довбак Богдан Іванович. Модернізація системи захисту інформації в Моторвагонному депо Королево.
15:30	Кава брейк
15:45	Ковальов Олександр Олександрович. Небезпека інфікування ПК програмами типу Spyware.
16:00	Балог Павло Павлович. Ренгенофотоелектронні спектри і оптимізація одержання високочистих плівок на основі кристалічного β-$GeS_{2.}$
16:15	Левицька Євгенія Сергіївна. Імітаційне моделювання кристалізації сплаву $(Ge_{40}S_{60})_{100-x}Bi_x$.
16:30	Цисельська Катерина Віталіївна. Створення антивірусної програми для операційної системи Windows, з використанням сигнатурного методу захисту та хеш-функції MD5.
16:45	Ігнатко Марія Іванівна. IT-інновації в управлінні розвитком агропромислового виробництва.
17:00	Щербанич Віталій Віталійович. Дослідження процесу механічного подрібнення кристалів SbSJ.
17:15	Ухач Тетяна Іванівна. Програма обміну повідомленнями з трирівневою системою захисту.
17:30	Балога Михайло Тарасович. Фізичні властивості біоінформаційних молекул.
17:45	Мірошина Юлія Володимирівна. Вплив сторонніх факторів на систему голосової автентифікації для Android.
18:00	Кутканич Володимир Юрійович. Захист інформації у апаратно-технічних приміщеннях на спорткомплексі «Минай».
18:15	Барна Іван Юрійович. Спектральна залежність температурного приросту показника заломлення стекол системи As-S.
18.30	Пасіка Марк. Захист інформації від несанкціонованого доступу у філії

	медичного центру «Інтерсоно».
18:45	Бонкало Василь Анатолійович. Захист інформації в системах мобільного зв'язку та написання додатку для шифрування текстової інформації методом Rijndael.
19.00	Кравчук Олексій. Електрофотографічні дослідження тонких плівок на основі аморфного селену.
19.15	Гевці Давид Олександрович. Еволюція Раман спектрів склоподібного GeS_2 при технологічному модифікуванні.
19.30	Мачужак Богдан Олександрович. Проектування захищеного оптоволоконного каналу зв’язку.
19.45	Савчин Андрій Михайлович. Спектри комбінаційного розсіювання скловидного тетраборату літію, активованого оксидом тербію.
20.00	Мицька Михайло Мирославович. Низькотемпературна теплопровідність і бозонний пік склоподібного As_2S_3.
20.15	Урочисте закриття конференції, оголошення переможців, вручення нагород.

КАФЕДРА ТВЕРДОТІЛЬНОЇ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДВНЗ „УжНУ”

УКРАЇНСЬКЕ ФІЗИЧНЕ ТОВАРИСТВО

АКАДЕМІЯ ТЕХНОЛОГІЧНИХ НАУК УКРАЇНИ

7 листопада 2019

УЖГОРОД

V НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

"ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ЖИТТІ СТУДЕНТІВ ТА МОЛОДИХ НАУКОВЦІВ ЗАКАРПАТТЯ"

7 листопада 2019 року

ТЕЗИ ДОПОВІЕЙ

УЖГОРОД - 2019

ВЕБ-СКРАПІНГ: АВТОМАТИЗОВАНИЙ ЗБІР ІНФОРМАЦІЇ З WEB-РЕСУРСІВ

Буковецький Василь Іванович

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54,

аспірант кафедри ТЕІБ

Веб-скрапінг — процес перетворення призначених для перегляду людиною веб-сторінок у структуровані дані.

Веб-сторінки будуються за допомогою текстових мов розмітки (HTML та XHTML) і часто містять велику кількість корисних даних у текстовій формі. Однак більшість веб-сторінок призначені для кінцевих користувачів, а не для зручності автоматичного використання.

Основними видами веб-скрапінгу є:

- Ручне копіювання
- Регулярні вирази
- HTML-парсинг
- DOM-парсинг
- Розпізнавання семантичних анотацій

Легальність використання автоматичних методів збору варіюється від країни до країни - так, в США та Європейському Союзі в деяких випадках суд визнавав використання веб-ресурсу як цілком законне, а в деяких ні.

Неправильна робота розробниками веб-ресурсів з базами даних SQL часто дозволяє значно спростити скрапінг. Так, дуже частою помилкою є відсутність екранізації wildcard-символів у виразі LIKE в запитах пошуку. Також дуже часто можна зустріти відсутність перевірки в запиті на сервер поля з кількістю елементів, що виводяться на екран.

Багато сучасних веб-сайтів та сервісів розділяють бек-енд та фронт-енд, де фронт-енд додаток з’єднується з сервером за допомогою API. Це зводить задачу до звичайного підключення та структуризації даних.

СТВОРЕННЯ ПРОГРАМНОГО КОМПЛЕКСУ ШИФРУВАННЯ ІНФОРМАЦІЇ В ОПТОВОЛОКОННИХ КАНАЛАХ ЗВ'ЯЗКУ МЕТОДОМ RSA

Бібен Іван Едуардович

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54

студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

Інформація, яка передається через комп'ютерну мережу, проходить через певну кількість шляхів, перш ніж досягне пункту призначення. Одним з головних є оптоволоконний канал зв'язку, через який проходить найбільше даних. Основними проблемами, що виникають при передачі інформації, є: перехоплення зловмисником інформації, її модифікація та підміна авторства.

Єдиним засобом захисту каналу великої протяжності при передачі інформації є криптографічний захист. Для вирішення цієї проблеми була розроблена програма шифрування текстової інформації на основі алгоритму RSA з певними модифікаціями. Використання програми зменшує необхідність у шифруванні каналу при передачі повідомлення, так як дані шифруються та розшифровуються на кінцевих вузлах.

У програмі використаний принцип асиметричного шифрування, реалізований на мові програмування Java. При передачі конфіденційної інформації між двома співрозмовниками у кожного генерується по парі ключів - відкритий та закритий ключ. Ключі є взаємозв'язними, математично залежні одне від одного. Для того щоб уникнути можливої лобової атаки (підбору ключів зловмисником) ключі вибираються великої довжини, а час на їх підбір зловмисником сягне декількох років. Повідомлення зашифровується відкритим ключем отримувача та розшифровується його особистим закритим ключем.

Модифікаційною складовою програми є впровадження в неї розмежування повідомлень за критеріями важливості: - 1 рівень – секретно, 2 рівень – цілком таємно, 3 рівень – особливої важливості, та збільшення ключа

шифрування. При передачі повідомлення користувачем вибирається цей параметр. Відповідно до критерія важливості будуть формуватися ключі шифрування: 512 bit, 1024 bit, 3072 bit. Чим більший ключ, тим довше буде проходити процес шифрування/розшифрування, але ризик розшифрування інформації, перехопленої зловмисником, зводиться до неможливого, підвищується криптостійкість.

Створення програмного комплексу вирішило проблему захищеності каналу зв’язку й може бути використано на інших каналах у разі потреби. В подальшій перспективі програмний комплекс може бути реалізований у технічних засобах та впроваджений як проміжна ланка мережі.

WEB-ОРІЄНТОВАНИЙ ІНТЕРФЕЙС ВІДДАЛЕНОГО ДОСТУПУ ДО ВІРТУАЛЬНОЇ НАВЧАЛЬНОЇ ЛАБОРАТОРІЇ

Гайсак Андрій Іванович

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54,

студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

У період стрімкого розвитку комп'ютерної техніки та технологій в цілому фізики, як спеціалісти, брали чималу участь в прогресі цієї сфери.

Так, наприклад, після появи перших мов програмування фізики не лише активно користувались ними, але й модифікували їх або ж розробляли свої варіанти. Одною із таких є мова програмування Фортран. Фортран - імперативна мова програмування загального призначення, яка особливо підходить для інтенсивних чисельних та наукових обчислень. Розроблена корпорацією IBM в 1950-х роках в університетському містечку на півдні Сан-Хосе (Каліфорнія) для потреб наукових та інженерних проектів. Фізики в свій час писали чималу кількість програм на Фортрані, які допомагали їм з обчисленнями, але після появи об'єктно-орієнтованих мов програмування прогрес взяв своє. Більшість науково-обчислювальних структур перейшли на використання сучасніших мов програмування, таких як C++. Відповідно всі програми, які були раніше написані на Фортрані, потрібно було переписати на C++. Звичайно ж деяка частина з них була переписана, але левова частка програм залишились незмінними. Отже, було б непогано використовувати ці програми й нині, без потреби їх повного перепису. Та ще й використати можливості сучасних інтернет технологій.

Актуальність: Завдяки даній роботі можна уникнути переписування тисячі програм на нову мову програмування та реалізувати простий і зручний метод користування ними.

Мета даної роботи: Реалізувати доступ до програм, написаних на Фортрані через звичайний веб-браузер, без потреби встановлення їх на своєму пристрої та витрачання його ресурсів. Створити веб-інтерфейс, який би

дозволяв віддалено користуватися такими програмами в наукових та навчальних цілях.

Завдання роботи:

- Зібрати ПК, на якому будуть знаходитись програми для науки та навчання та на якому будуть відбуватись обчислення
- Встановити на нього ОС Linux Ubuntu Server
- Налаштувати APACHE
- Встановити тестову програму на мові програмування Фортран для обрахунку певних даних
- Написати скрипт на мові програмування Perl, який буде запускати нашу програму та обмінюватись даними з веб-сторінкою
- Створити веб-інтерфейс як спосіб підключення та взаємодії з сервером
- Захистити сервер від небажаних атак за допомогою OpenVPN open source project

У результаті виконання даної роботи я отримав робочий прототип макету віртуальної лабораторії. Програми для обрахунків знаходяться і виконуються на сервері, який був зроблений і налаштований мною вручну. Всі налаштування були підібрані так, щоб максимально відповідати вимогам проекту. Також під час створення проекту велика увага надавалась швидкодії всіх процесів.

Для взаємодії користувача з програмами мною було створено веб-інтерфейс. Його основною задачею є максимально швидко та просто надавати доступ до функцій програм та візуалізувати ввід та вивід даних для користувача.

Поєднати переваги веб-інтерфейсу та переваги обрахунку даних на сервері вдалось за допомогою скрипту написаного мною на мові програмування Perl. Щодо безпеки, то захист враховувався на всіх етапах створення.

Завдяки даній роботі можна уникнути переписування тисячі програм на нову мову програмування та реалізувати простий і зручний метод користування ними.

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВЕРИФІКАЦІЇ ВТОРИННОЇ АВТЕНТИФІКАЦІЇ

Шкомар Юрій Андрійович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54,
студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

Як і в усіх системах передачі даних, важливою характеристикою є безпека інформації, що передається, в якій необхідно бути впевненим в тому, що повідомлення дійшло до адресата без перехоплення і змін. Звідси випливають вимоги, що пред'являються до процесу забезпечення інформаційної безпеки (ІБ). ІБ повинна забезпечувати цілісність, доступність і конфіденційність інформації.

Під поняттям конфіденційності ми розуміємо те, що наша особиста або ділова інформація не повинна бути доступна третім особам. При використанні інформаційних систем (ІС), що мають на увазі будь-які взаємини між декількома суб'єктами, ми хочемо, щоб ніхто не міг робити ніяких дій від нашого імені. Для вирішення цих завдань використовуються складні криптографічні системи, що забезпечують надійне шифрування даних, і створення непідробних цифрових підписів.

З розвитком систем забезпечення інформаційної безпеки фактор неправильної роботи ІС відходить на другий план. Більшість загроз ІБ пов'язані з людським фактором. З більшістю ІС може працювати кілька користувачів, а, отже, необхідно розмежувати доступ до ІС. Для цієї мети використовують різні методики поділу доступу. Поділ доступу має на увазі три процедури взаємодії між суб'єктом і системою: ідентифікація, автентифікація і авторизація. На етапі ідентифікації відбувається визначення особистості, під час автентифікації відбувається підтвердження особи, а при проведенні авторизації з'ясовується до яких ресурсів ІС отримує доступ конкретний користувач. Найбільш слабкою ланкою в даній ланцюжка є автентифікація. При зломі системи автентифікації

зловмисник буде сприйнятий системою як легальний користувач і йому будуть розкриті дані, що зберігаються в ІС. На етапі автентифікації відбувається взаємодія між людиною і комп'ютерною системою. Тому важливим є вибір захищеного способу автентифікації.

Завдяки даній роботі можна досягти захисту персональних даних з різних підсистем в одному додатку на смартфоні. Отже, метою даної роботи є реалізація мобільного додатку, захищеного сервера та їх взаємодія для захисту персональних даних користувача в процесі логінізації до будь-якої підсистеми.

Завдання роботи:

- Проаналізувати вже існуючі додатки
- Визначити недоліки вже створених автентифікаторів
- Проаналізувати існуючі методі та алгоритми створення програмного забезпечення автентифікації
- Вибрати найбільш підходящі алгоритми та методи створення програмного забезпечення
- Створити сервер для генерування, обробки та зберігання даних
- Створити мобільний додаток-автентифікатор
- Написати захищений алгоритм передачі даних між сервером та мобільним додатком

При виконанні даної роботи було проаналізовано наявні на ринку авфтенифікатори та їх недоліки, розглянуто найбільш підходящі методи та алгоритми для створення власного додатку-автентифікатора для захисту персональних даних.

ЗАГЛУШУВАЧ НА БАЗІ ПЛАТИ ARDUINO NANO ДЛЯ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ

Пішковцій Марія-Ольга Іванівна

Державний вищий навчальний заклад «УжНУ»
88000, Ужгород, вул. Волошина, 54
студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

Згідно тенденціям розвитку суспільства найбільш поширеним ресурсом є інформація, отже, її цінність, постійно зростає. За досить тривалий період свого розвитку людство накопичило величезний ресурс знань про способи і засоби ведення розвідки. Спочатку цей досвід носив в основному військовий характер, але потім його реалізація стала можлива і розповсюдилась на звичайних користувачів. Одним з основних способів ведення розвідувальних дій є отримання доступу до каналів передачі інформації. Інформація стала не тільки найважливішою сферою міжнародної співпраці, а й об'єктом суперництва. Проблеми у сфері інформаційної безпеки загострюються внаслідок політичного й економічного протиборства держав. Це стало актуальним у зоні забезпечення інформаційної безпеки України.

Оскільки розголошення деякої інформації часто призводить до негативних наслідків для її власника питання захисту інформації від несанкціонованого її отримання стає все актуальнішим. На сьогодні існує безліч технічних каналів витоку інформації, різновидом яких є канали витоку мовної інформації. При побудові надійної системи захищеності інформаційних ресурсів необхідно застосовувати комплексний підхід, враховуючи всі можливі варіанти витоку інформації. Тому можна вважати, що проблема захисту мовної інформації є доволі критичною і потребує пошуку найкращого рішення.

Одним із таких рішень може стати заглушувач на базі Arduino Nano для захисту мовної інформації. Для того щоб розробити такий унікальний пристрій потрібно: алгоритм і програмне забезпечення в середовищі Arduino IDE на мові програмування C++; плата Arduino Nano v3.0; модуль NE555. Результатом

тестування заглушувача стало можливість отримати шістдесяти відсоткове зашумлення мовної інформації на відстані 2 м, що є мінімальним порогом щодо отримання виразності розмови. За допомогою спеціального обладнання ця відстань зменшується на 0,5 м і 40%.

Отже, керуючись результатами дослідження роботи можна прийти до висновку, що заглушувач на базі Arduino Nano може використовуватися для захисту мовної інформації від витоку акустичними каналами.

ДОДАТОК ДЛЯ ВИЯВЛЕННЯ ТА ЗНЕШКОДЖЕННЯ ШПИГУНСЬКОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ У ПЕРСОНАЛЬНИХ КОМП'ЮТЕРАХ

Гелетей Йосип Йосипович

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54,

студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

Нові потенційні помилки щодо безпеки програмного забезпечення та різні форми шкідливого програмного забезпечення щодня загрожують цілісності наших даних. Більшість із цих загроз існують вже тривалий час, але розвиток нових технологій, і, відповідно нових методів боротьби та захисту інформації, спонукає зловмисників постійно розвивати вміння в розробці шкідливих програм, від чого вони стають небезпечнішими для електронних систем і важчими для виявлення.

Метою даної роботи є розробка методів щодо виявлення шпигунської програми класу кей-логгер, з функцією екранного шпигуна.

Методами дослідження є аналіз поведінки ПК, який містить шпигунську програму, моніторинг процессів та зміни продуктивності апарату.

Для досягнення мети необхідно виконати такі завдання:

1. Провести аналіз функціонування та класифікації шпигунських програм, способів їх поширення.
2. Визначити та дослідити загальної методології та алгоритми виявлення та знешкодження шпигунських програм, виходячи з особливостей їх функціонування.
3. Розробити засіб моніторингу системи, беручи до уваги інформацію про навантаженість основних апаратних компонентів ПК, та аномалії, пов'язані з даними процесами
4. Впровадити в рамках створеного спеціалізованого програмного забезпечення методів для виявлення процесів, що спричинюють аномальну поведінку апаратної частини ПК.

5. Надати користувачу кінцеві звіти про наявність шпигунської програми.

ДОДАТОК ДЛЯ ПОБУДОВИ СТРУКТУРНОЇ МОДЕЛІ ОБЛИЧЧЯ ЗА ДОПОМОГОЮ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ

Грабовчак Я. П.

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54,

студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

На сьогоднішній день широке розповсюдження відеокамер сприяє розвитку відеоаналітики. Дана технологія використовує компютерний зір для автоматичного збору інформації по обличчях з відеоканалів у реальному часі або з відеозаписів. Використовуючи структурну модель обличчя, можна розпізнати емоції, а відповідно і настрій певної особи або скупчення осіб. Тому розвиток даної технології може бути застосований для виявлення небезпеки при відеоспостереженні. Також може мати практичне застосування в системах контролю доступу та ідентифікації особи.

Прогрес в області штучного інтелекту і біометричних технологій, включаючи розвиток можливостей машинного навчання, призвів до підвищення точності та доступності комп'ютеризованих технологій розпізнавання облич і до їх ширшого розповсюдження. Тепер розпізнавання обличчя може відбуватися в великих масштабах і в більш складних умовах.

Для реалізації додатка використовуються відкриті програмні бібліотеки, створені на основі згорткових нейронних мереж, котрі з кожним днем стають більш потужними. Вони використовуються переважно для вирішення завдань комп'ютерного зору, але можуть застосовуватися і для роботи з аудіо чи іншими даними, які можна представити у матричному вигляді.

Розпізнавання емоцій означає можливість виділяти обличчя на зображеннях. За допомогою згорткових нейронних мереж можна виділяти людей або окремі частини тіла людини на фото або відео, для побудови їхніх скелетів, поз, структурних моделей. Даний підхід також застосовується для відеоаналітики.

МІНІМІЗАЦІЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФІЛІАЛУ БАНКУ "ПЕРШИЙ УКРАЇНСЬКИЙ МІЖНАРОДНИЙ БАНК" НА ОСНОВІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Сосна Андрій Борисович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54,
студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

Стрімкий розвиток інформаційних технологій, широке застосування засобів обміну інформацією, всеохоплююча комп'ютеризація всіх сфер життєдіяльності зумовлюють актуальність дослідження питань інформаційної безпеки інфраструктури. Забезпечення ефективного захисту інформації є надзвичайно актуальним і для установ банківської сфери, адже саме банки володіють конфіденційною інформацією про своїх клієнтів, захист персональних даних яких від спотворень, витоків та хакерських атак є однією з найважливіших задач банку. Під час аналізу діяльності підприємства і оцінювання портфелю ризиків, що впливають на цю діяльність, особливу увагу слід приділяти саме інформаційним ризикам, які виникають при роботі банку.

Проблемам аналізу та мінімізації ризиків, а також особливостям інформаційних ризиків присвячено ряд робіт вітчизняних авторів, але у представленій роботі розглядається мінімізація ризиків інформаційної безпеки, притаманних саме банківській діяльності. Таким чином, забезпечення інформаційної безпеки банківських установ є нагальною і актуальною проблемою їх функціонування, адже несе у собі потенціал збереження й ефективного використання фінансових та інформаційних ресурсів банків, своєчасного виявлення та нейтралізації реальних та потенційних ризиків.

На прикладі Першого Українського Міжнародного Банку проведено аналізу ризиків інформаційної безпеки та запропоновано заходи щодо мінімізації інформаційних ризиків в даному банку за допомогою комплексної системи захисту інформації.

РОЗРОБКА САЙТУ КАФЕДРИ ТВЕРДОТІЛЬНОЇ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЙОГО ЗАХИСТ ВІД DDOS-АТАК

Савенко Євген Володимирович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54,
студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

XXI століття - це століття інформаційних технологій. Відомо, що інформаційні технології (ІТ) зазнали глобального поширення у всіх галузях: від освіти і до медицини. Сьогодні успіх буде мати той заклад, який володіє найсучаснішими комп'ютерними технологіями.

Однією з найбільш популярних в ІТ є галузь веб-технологій, але створити правильний веб-сайт під вибрану галузь - це тільки півшляху до мети; інша половина – створення веб-сайту захищеним від зовнішніх загроз. Напевно немає такої людини, яка має доступ до глобальної мережі, не чула про веб-сайти, і не зіткнулася з проблемою доступу до них. Основною перевагою захищеного веб-сайту є цілодобовий доступ до нього і максимально чіткий алгоритм протидії DDoS-атакам. Оскільки кількість DDoS-атак на сайти не зменшується в наш час, а навпаки тільки збільшується, є актуальною розробка захищеного сайту для кафедри ТЕІБ, який може з даним видом атак боротися.

Розроблений веб-сайт містить: захищену панель адміністратора для додавання новин та анонсів; використання системи керування контентом, яка найменш піддавалася злому; «легкий» та гнучкий код, який не навантажує сайт; адаптацію під будь-який екран користувача; мінімальний час відклику сайту; впровадження скрипту фільтрації. Забезпечує користувачу простий та зручний інтерфейс; швидкий та захищений доступ до інформації - навчального матеріалу; новин, складу кафедри; ознайомлення з науковими працями студентів, студентського життя; контактної інформації та розділу з актуальною інформацією для абітурієнтів. Робота користувача на сайті не залежатиме від того, чи сайт працює в штатному режимі чи бореться з DDoS-атакими.

ОСНОВНІ ПРИНЦИПИ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ КОМПЛЕКСНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ «ОКТАВА-ФІНАНС»

Сивуля Вадим Миколайович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54,
студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

У сучасному світі інформаційний ресурс став одним із найпотужніших важелів економічного розвитку. Знання потрібної інформації в потрібний час та в потрібному місці – запорука успіху в будь-якій сфері бізнесу.

Інформаційні технології присутні в кожному аспекті повсякденного життя. Головні проблеми у забезпеченні їх безпеки пов’язані з інформацією та технологіями її отримання, обробки, накопичення, збереження, аналізу та використання. Жодну організацію неможливо уявити без використання новітніх комп’ютерних технологій: від автоматизації окремих робочих місць до побудови фірмових розподілених інформаційних систем.

Широке застосування інформаційних технологій призводить до появи багатьох негативних аспектів, а саме до розширення сектору тіньової економіки, шахрайства, неконтрольованих та нефіксованих дій суб’єктів, небезпеки оприлюднення приватної інформації, росту числа кіберзлочинів. Тому питання захисту інформації у фінансовій сфері набуває неабиякої актуальності.

Суть інформаційної безпеки у діяльності фінансової установи полягає в ефективному забезпеченні її безперебійної роботи. Інформаційна безпека повинна мінімізувати збитки від подій, що несуть загрозу для підприємства, і звести їх наслідки до прийнятних [1]. Необхідність розробки систем захисту інформації закладається у основи планування й управління в фінансовій установі.

Товариство з обмеженою відповідальністю Фінансова компанія «Октава-Фінанс» здійснює валютно-обмінні операції, пов'язані з готівковою іноземною валютою та наданням кредитних послуг. Фінансова установа має в наявності програмні та програмно-технічні комплекси для захисту інформації на підприємстві.

За результатами досліджень на підприємстві нами було встановлено можливі загрози витоку інформації [2] і показано вразливість системи її захисту. Надано рекомендації щодо вдосконалення технічних засобів захисту інформації і безпеки вказаної фінансової компанії.

1. Комплексні системи захисту інформації: навчальний посібник/ [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2017. – 120 с.

2. Русіна Ю. О., Острякова В. Ю. Удосконалення системи управління інформаційною безпекою на підприємстві // Міжнародний науковий журнал "Інтернаука". — 2017. — №14, с.135-139.

КВАНТОВО-ХІМІЧНЕ МОДЕЛЮВАННЯ ПОВЕРХНІ TiO_2 У СЕРЕДОВИЩІ QUANTUM ESPRESSO

Штец Володимир Юрійович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54,
студент магістратури 2 року навчання

Квантово-хімічне моделювання та розрахунки чистої поверхні кристалу TiO_2 [110] проведено в рамках теорії функціоналу густини з використанням програмного пакету QUANTUM ESPRESSO. Ця програма використовує базис плоских хвиль та псевдопотенціалів та ефективний алгоритм швидкого перетворення Фур'є (для перетворення хвильових функцій між реальним та оберненим простором), зонний метод спряженого градієнту та алгоритм спряженого градієнту потенціала, що дозволяє визначити самоузгоджений потенціал, повну енергію та оптимізувати геометричну конфігурацію системи

Фізичні властивості були отримані на рівні теорій DFT (теорії, що використовує гібридний обміннокореляційний функціонал електронної густини в узагальненому градієнтному наближенні B3LYP (Becke, Lee, Yang, Parr)) з використанням гаусівського набору базисних функцій [O 8-411 (d1), Ti 86-411 (d41)].

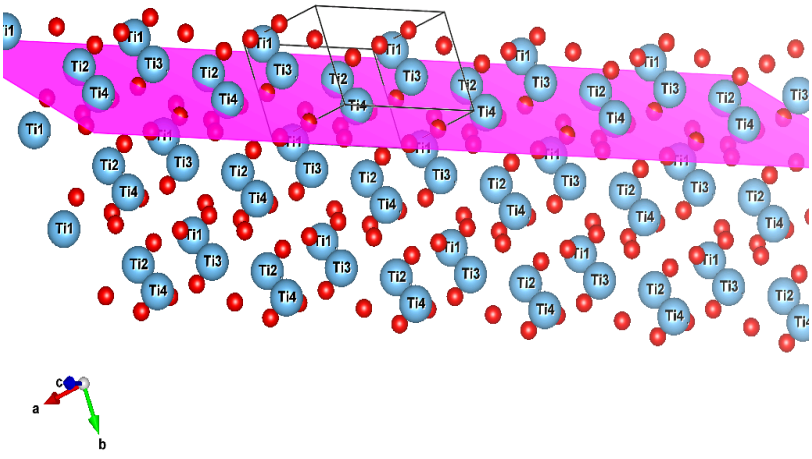


Рис. Модельна поверхня для TiO_2, напрямок [110]

Набори базисних функцій володіють тією властивістю, що всі функції з даного функціонального простору (з урахуванням деяких обмежень) можуть бути представлені як їх лінійна комбінація. Наприклад, будь-яка аналітична функція одного аргументу може бути розкладена в суму статичних функцій з різними коефіцієнтами, тобто розкладена в ряд Тейлора. Якщо в якості базисних обрані синусоїдальні функції, то розкладання по них є перетворення Фур'є і т. д.

Розрахувавши мінімальну енергію елементарної комірки кристалу TiO_2 [110], а також міжатомні кути і відстані, на основі аналізу результатів моделювання виявлено, що досліджуваний кристал є стабільним з точки зору структурної геометрії; отримані результати добре узгоджуються з експериментальними та літературними даними.

НЕБЕЗПЕКА ІНФІКУВАННЯ ПК ПРОГРАМАМИ ТИПУ SPYWARE

Ковальов Олександр Олександрович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54,
аспірант 3 року навчання, спеціальність 104 «Фізика та астрономія»

Spyware - це тип шкідливого ПЗ, яке заражає комп'ютер або мобільний пристрій з метою збору інформації про користувача, включаючи сайти, які він відвідуєте, файли, що завантажуються, імена користувачів та паролі, платіжну інформацію та електронні листи, що відправляються і отримуються.

Шпигунське ПЗ важко виявити, оскільки воно може бути як окремою програмою, так і вбудованим модулем до іншої програми.

Яким би способом шпигунське ПЗ не проникало на комп'ютер, метод роботи, як правило, один і той же - воно приховано працює у фоновому режимі, збираючи необхідну інформацію про користувача або контролюючи ПК, щоб викликати шкідливі дії. І навіть якщо користувач виявить його небажану присутність у системі, Spyware не поставляється з функцією легкого видалення.

У більшості випадків функції шпигунських програм залежать від намірів їх авторів. Нижче наведені приклади найбільш поширених типів шпигунських програм, що *класифікуються* відповідно до їх функцій:

- *Програми для крадіжки паролів* – це програми, що розробляються для збору паролів на заражених комп'ютерах. Зокрема, вони можуть збирати облікові дані, які користувач вводить у браузері, облікові дані для входу в систему, а також інші паролі. Отримані відомості можуть зберігатися на зараженому комп'ютері - в місці, визначеному самою програмою, або передаватися на віддалений сервер для подальшої обробки;
- *Банківські троянські програми* - це додатки, що розробляються для збору облікових даних фінансових установ. Вони використовують вразливості в системі захисту браузерів, щоб оновити веб-сторінки, змінювати контент транзакцій або вставляти в потік даних додаткові транзакції, залишаючись при цьому абсолютно невидимими як для користувача, так і для основного веб-

додатку. Ці програми також можуть передавати зібрані дані на віддалені сервери для подальшого вилучення;

- *Програми для викрадення даних* – це програми, які сканують заражені комп'ютери в пошуках різної інформації, наприклад імен користувачів, паролів, адрес електронної пошти, історії браузерів, файлів журналів, системних даних, документів, електронних таблиць чи інших файлі. Як і банківські троянські програми, програми для викрадення даних можуть використовувати вразливості в системі захисту браузерів, щоб збирати особисті дані користувачів на форумах і в онлайн-сервісах, а потім передавати отриману інформацію на віддалений сервер або зберігати її безпосередньо на зараженому ПК для подальшого вилучення;
- *Клавіатурні шпигуни, також відомі як системні монітори*, – це програми, що розробляються для стеження за діями користувача комп'ютера, наприклад за натисканнями клавіш, відвідуванням веб-сайтів, історією пошуку, обговореннями в електронній пошті, діалогами в чатах, а також за введеними обліковими даними системи. Зазвичай вони накопичують знімки екранів, запам'ятовуючи поточне вікно через певні інтервали часу. Клавіатурні шпигуни також збирають відомості про роботу системи, непомітно захоплюючи і передаючи зображення, аудіо- та відеофайли з підключених пристроїв. Вони навіть можуть накопичувати документи, які користувачі друкують на приєднаних до системи принтерах, а потім передавати ці документи на віддалені сервери або зберігати їх локально для подальшого вилучення.

Основною відмінністю програмних шпигунів у порівнянні з програмними вірусами є той факт, що для знаходження та знешкодження Spyware необхідно використовувати спеціалізоване ПЗ, яке не завжди входить до базового функціоналу антивірусної програми. Тому навіть наявність платної версії потужного антивірусного ПЗ не може гарантувати, що після сканування всіх системних файлів в ній не буде знайдено прихований програмний шпигун.

1. "Anti-Spyware". Total Technology Resources. July 28, 2016. Retrieved November 20, 2017.

2. SPYWARE ""Archived copy" (PDF). Archived from the original (PDF) on November 1, 2013. Retrieved February 5, 2016."

3. Basil Cupa, Trojan Horse Resurrected: On the Legality of the Use of Government Spyware (Govware), LISS 2013, pp. 419–428

4. "Microsoft Acquires Anti-Spyware Leader GIANT Company". December 16, 2004. Archived from the original on February 27, 2009. Retrieved April 10, 2009."

СУЧАСНІ ТЕХНОЛОГІЇ РОЗРОБКИ ОДНОСТОРІНКОВИХ ВЕБ-ДОДАТКІВ

Антосяк П. П.

ДВНЗ «Ужгородський національний університет»
математичний факультет,
доцент кафедри системного аналізу та теорії оптимізації

Половко І. І.

ДВНЗ «Ужгородський національний університет»
студент 4 курсу математичного факультету

Сьогодні веб-технології швидко розвиваються. Платформонезалежність та доступність веб-сайтів роблять їх дуже привабливими для розробників. Розвиток веб-технологій сьогодні дозволяє будувати не лише веб-сайти у звичайному сенсі цього слова – коли сайт складається зі статичних сторінок, а й дуже інтерактивні сайти – односторінкові веб-додатки, які можна називати повноцінними додатками. Такі веб-додатки вже становлять значну конкуренцію нативним додаткам, що змушує розробників створювати онлайн версії популярних додатків.

Односторінковий веб-додаток (*single-page application* (SPA)) – це концепція веб-сайту, що робить його інтерактивним й дуже схожим на звичайний додаток, зберігаючи при цьому всі переваги веб-сайту. Ідея SPA не є новою, вона почала з’являтися як тільки з’явилися JavaScript та AJAX і веб-сайти почали набувати динамічності будучи вже не лише статичними сторінками. Мабуть кожному розробнику сайтів рано чи пізно приходили в голову ідеї про сайт-додаток, який завантажується лише один раз, а все інше відбувається за рахунок сценаріїв та асинхронних запитів. Проте об’єм роботи, який треба було зробити не був вартий цього, адже для створення веб-сайту за концепцією SPA треба прикласти значних зусиль. Сьогодні полегшити розробку такого виду сайтів допомагає використання технологій, фреймворків та інструментів, що були для цього створені в останній час.

З метою дослідження та аналізу можливостей сучасних фреймворків для розробки односторінкових веб-додатків проведено збір теоретичних відомостей про концепцію односторінкового веб-додатку та типові особливості їх архітектури. У доповіді наводиться огляд існуючих SPA додатків та технологій, що були використані при їх розробці; огляд інструментів та фреймворків, що використовуються при їх розробці; демонстрація можливостей та переваг фреймворка Angular на прикладі реально існуючого та діючого проекту.

1. Single page apps in depth. – Режим доступу: http://singlepageappbook.com/goal.html – Дата доступу: 01.11.2019.
2. Офіційний сайт Angular. – Режим доступу https://angular.io/ – Дата доступу: 01.11.2019.

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ КРИСТАЛІЗАЦІЇ СПЛАВУ $(Ge_{40}S_{60})_{100-x}Bi_x$

Левицька Є. С., Горват Г. Т.

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

Темп науково-технічного прогресу дотримується ціноправніх пошуків нових матеріалів із різними характеристиками та індивідуальними властивостями. Відсутність теоретичних моделей, що дозволяють виконати обчислювальний експеримент, пояснюється недоліками традиційних підходів теоретичного опису фазових перетворень, для яких притаманне одночасна поява і зростання великого числа зародків нової фази, їх складна форма і взаємодія. В зв'язку з цим є дуже важливими використання в науковому експерименті сучасних моделей структурних характеристик, прогнозованих властивостей і процесів, які пов'язані з отриманням нових матеріалів.

Метою даної роботи є дослідження процесу структуроутворення сплаву $(Ge_{40}S_{60})_{100-x}Bi_x$ при гомогенній кристалізації з використанням імітаційної моделі кристалізації бінарного сплаву з евтектикою.

Розглядаючи кристалізацію чистого металу або бінарного сплаву можна виділити основні фізичні процеси, що визначають її хід. По-перше, це теплопередача, що відбувається в об'ємі розплаву під впливом зовнішніх чинників [1]. Тому основним блоком, що задає динаміку роботи моделі, є блок визначення температурного поля упродовж всього процесу. В його основу покладено рівняння теплопровідності Фур'є з граничними умовами третього роду. Другим найбільш істотним фізичним явищем в даному випадку є процеси, які пов'язані з перерозподілом компонентів сплаву. Для опису дифузії компонентів в рідині зручно використовувати рівняння Фіка, яке з математичної точки зору є аналогічним рівнянню теплопровідності [2]. Граничні умови в цьому випадку припускають відсутність обміну речовиною на межах системи. Варіювання умовами кристалізації та її параметрами приводить до відповідних змін структури матеріалу. Відповідно, обчислювальний експеримент за

допомогою підсистеми імітаційного моделювання структуроутворення при кристалізації надає можливість досліджувати вплив температури та кількості модифікатора на процес фазового перетворення, а саме на зміну основних параметрів кристалізації. Причому ці дослідження мають кількісний характер, що зробити в натурному експерименті з металом практично неможливо.

Показано, що при наявності модифікатора кристалізація невеликої за розмірами системи набуває об'ємного характеру за рахунок наявності твердих частинок в об'ємі рідкого напівметалу, які є осередками кристалізації.

1. Rivier N. Structure of glasses from a topological viewpoint // Proc. 2nd International Conf. – Cambridge (UK). – 1982. – p.517–538.
2. Бялік О.М., Доний О.М., Голуб Л.В. Прогноз властивостей металів і сплавів методом комп'ютерного термічного аналізу. Препринт.- Київ.- "Політехніка".- 2005.- 116 с.

СТВОРЕННЯ АНТИВІРУСНОЇ ПРОГРАМИ ДЛЯ ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS З ВИКОРИСТАННЯМ СИГНАТУРНОГО МЕТОДУ ЗАХИСТУ ТА ХЕШ-ФУНКЦІЇ MD5

Цисельська Катерина Віталіївна

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54,
студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

Людство перейшло в епоху, коли інформаційне суспільство стало розвинене як ніколи. \Ми все більше і більше використовуємо інформаційні технології та телекомунікаційні системи у всіх сферах нашої життєдіяльності та у державній сфері. Однак варто розуміти, яку небезпеку несуть за собою ці технології. На сьогоднішній день жертвами «хакерів» та комп'ютерних вірусів стають не лише звичайні користувачі, але й цілі держави. Тому виникає потреба в швидкому реагуванні на нові загрози та віруси.

Сигнатурний метод захисту полягає у проведені сигнатурного аналізу, що є найбільш відомим методом виявлення вірусів та використовується практично в усіх сучасних антивірусних програмах. Сам по собі сигнатурний аналіз здійснює перевірку файлів на наявність у них сигнатур вірусів, що зберігаються в антивірусній базі (в сучасних антивірусах вона постійно потребує оновлення). Основною перевагою данного методу є стовідсоткова імовірність виявлення вірусу при правильній реалізації вірусної сигнатури.

Розроблена на основі цього методу антивірусна програма дозволить відслідковувати та знищувати віруси у режимі реального часу. На відміну від вже існуючих антивірусів, користувачу не доведеться чекати офіційного оновлення антивірусної бази від розробників; при володінні певними навичками користувач може змінювати та задавати сигнатури сам, що дозволить швидше реагувати на загрози та уникнути втрат.

ІТ-ІННОВАЦІЇ В УПРАВЛІННІ РОЗВИТКОМ АГРОПРОМИСЛОВОГО ВИРОБНИЦТВА

Ігнатко Марія Іванівна

ДВНЗ «Ужгородський національний університет»,
аспірант кафедри економіки і підприємництва

Агропромисловий комплекс являє собою одну із найважливіших ланок національного господарства України. Значення аграрної сфери не тільки у забезпеченні потреб людей у продуктах харчування, але в істотному впливі на зайнятість населення й ефективність усього національного виробництва. Частка агропромислового виробництва станом на 2018 рік становить 10% загального обсягу ВВП та складає 36,9% експорту України [1, с.330]. До десятки країн, до яких найбільше експортується українська сільськогосподарська продукція, увійшли Індія (12,1%), Єгипет (6,4%), Китай (6,2%), Нідерланди (5,9%), Іспанія (5,1%), Туреччина (5,0%), Італія (4,9%), Іран (3,8%), Польща (3,6%), Білорусь (3,5%) [2].

На сьогоднішній час українські підприємства агропромислового виробництва, які активно застосовують інновації, ні в чому не поступаються іноземним конкурентам, а інколи їх і перевершують. Тобто, в Україні є приклади успішного освоєння інновацій підприємствами.

Перший рейтинг найбільш інноваційних компаній України опублікував журнал «Forbes», який формував його із врахуванням ряду чинників: це повинні були бути саме українські інноваційні підприємства, а не закордонні представництва; оцінювався безпосередній внесок компанії в розвиток власних інновацій; продукція компанії розглядалася з точки зору її унікальності та застосуванні інноваційних технологій при її виробництві; аналізувалися масштаби інновацій підприємства, здатність компанії посідати конкурентні позиції на ринку з їх допомогою; досліджувалась здатність інновації викликати попит з боку конкурентів і бажання копіювати в тій чи іншій формі. До Топ-20 цього рейтингу ввійшли п’ять агропромислових компаній (табл.1).

Таблиця 1

Позиції агропромислових підприємств у рейтингу найбільш інноваційних компаній України за версією журналу «Forbes» [3]

Місце в загальному рейтингу	Назва компанії	Індекс інноваційності
8	МХП ("Миронівський хлібопродукт")	54,2
15	"Нібулон"	43,8
18	"Сварог Вест Груп"	41,7
19	AgriLab	40,4
20	"Кернел"	33,3

Зберігати лідерство у галузі даним підприємствам вдається завдяки поширенню та впровадженню інновацій: farm management, систем точного землеробства, систем дистанційного зондування землі, систем GPS-моніторингу транспортних засобів, геоінформаційних систем управління агровиробництвом, автоматизації виробничих процесів накопичення баз даних, структуруванню і аналізу інформації, супутникового моніторингу, використання безпілотних літальних апаратів, використання автоматичних пробовідбірників, діджиталізації управління полем, інноваційній логістиці, ефективній аналітиці та прийнятті раціональних управлінських рішень з використанням інноваційних технологій тощо.

Отже, провідні компанії, що займаються рослинництвом та тваринництвом, активно шукають та впроваджують високоякісні інноваційні рішення, які здатні підвищити ефективність та продуктивність діяльності. Над пошуком інновацій працюють селекціонери, біологи, технологи, та інші професіонали. І далеко не останнє місце в даному списку займають ІТ-спеціалісти, чиї рішення за останні десятиліття докорінно змінили та продовжують змінювати діяльність багатьох агропромислових компаній.

1. Hotra V., Ihnatko M. Features of innovative development of Ukrainian agro-inductrial production management/ Scientific development and achievements. – Sciemcee Publishing. – London. – 2018. – p.329-337.

2. Офіційний сайт Державної служби статистики України [Електронний ресурс]. – Режим доступу: http://www.ukrstat.gov.ua/

3. Forbes: Врятувати майбутнє (перший рейтинг найінноваційніших компаній України) [Електронний ресурс]. – Режим доступу: [https://www.agrilab.ua/forbes-vryatuvaty-majbutnye-pershyj-rejtyng-najinnovatsijnishyh-kompanij-ukrayiny/

ДОСЛІДЖЕННЯ РОЗМІРІВ МЕХАНІЧНО ПОДРІБНЕНИХ КРИСТАЛІВ СУЛЬФОГАЛОГЕНІДА СУРМИ

Щербанич В. В., Пинзеник В. П.

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

Халькогалогенід сурми (SbSI) є напівпровідниковим сегнетоелектриком з температурою фазового переходу при кімнатній температурі (T≈22^{0}C), високою діелектричною проникністю, високим електро-оптичним коефіцієнтом, фотопровідністю з максимом фотоструму між 6300 – 6400 Å, та п'єзоефектом.

Метою даної роботи полягає у дослідженні властивостей ниткоподібних нанокристалів SbSI, виготовлених механічним подрібненням за допомогою кулькового млина.

Для визначення розмірів одержаних нанокристалів використовувся рентгенодифракційний аналіз. Середній розмір нанокристалів визначався з уширення рентгенодифракційних ліній за формулою Шеррера:

$$D = \frac{K\lambda}{\Delta(2\theta)\cos\theta_0}$$

де D – діаметр частинок, λ – довжина хвилі рентгенівського випромінювання, θ_0 – дифракційний кут, Δ(2θ) – повна ширини дифракційного піку на половині висоти.

Результати дослідження розмірів нанокристалів за допомогою електронної мікроскопії показали, що розподіл розмірів нанокристалів має гауссову форму з максимумом поблизу 70 нм і чітко вираженим піком поблизу 50 нм. Із збільшенням часу помолу пік максимуму гауссового розподілу наближається до цього краю, але нанокристалів з меншими розмірами виявлено не було. Ймовірним поясненням цього явища може бути те, що при розмірах ~50 нм механічна міцність нанокристалів стає максимальною, тобто кристалічна структура нанокристалів стає майже ідеальною і бездефектною.

Розміри нанокристалів одержані за формулою Шеррера та прямих електронно-мікроскопічних досліджень відрізняються вдвічі, що можливо пояснюється впливом поверхневого натягу.

ВПЛИВ СТОРОННІХ ФАКТОРІВ НА СИСТЕМУ ГОЛОСОВОЇ АВТЕНТИФІКАЦІЇ ДЛЯ Android

Мирошина Юлія Володимирівна

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54,
студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

Актуальність роботи випливає з постійного зростання кількості володарів облікових записів на мобільних платформах Android та розповсюдженості використання в системах захисту біометричних даних людини, а також постають все нові задачі для запобігання витоку конфіденційної інформації через загрози пов'язані з несанкціонованим доступом до профілів користувачів.

Метою даної роботи є визначення рівня впливу сторонніх факторів на голосову автентифікацію користувачів на мобільних платформах Android.

Методами дослідження є аналіз та порівняння методів впливу сторонніх факторів на процес автентифікації користувачів.

Для досягнення мети були виконані завдання: проведення аналізу методів автентифікації користувачів, досліджено їх переваги та недоліки при практичному застосуванні. Для дослідження була обрана голосова автентифікація особи і для розробки програмного забезпечення були обрані мова програмування C#, основним середовищем розробки було обрано Visual Studio 2018, допоміжним середовищем були емулятор Android NoxPlayer2 версії 5.0.0.0 та Xamarin; охарактеризовані локалізовані завади, які зустрічаються в повсякденному житті: зміни голосу користувача (крик, хрипота, виспівування, прискорення і уповільнення голосу); вимовляння фраз з фоновим ефірним шумом; автентифікація з сильним шумом, на тлі гучного звуку автостради та запис фраз з фоновим музичним шумом, що можуть впливати на систему голосової автентифікації; дослідження ступеню впливу зазначених завад на автентифікацію особи дало змогу визначити із завад найбільш (вимовлення паролю із ефірним шумом) та найменш (вимовлення паролю звичайним голосом та з музичним шумом) впливові на систему голосової автентифікації.

ЗАХИСТ ІНФОРМАЦІЇ У АПАРАТНО-ТЕХНІЧНИХ ПРИМІЩЕННЯХ НА СПОРТКОМПЛЕКСІ «Минай»

Кутканич Володимир Юрійович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54,
студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

Актуальність роботи випливає з постійного зростання інтересу до методів та засобів, які допомагають здобувати високі досягнення у спорті та розвитку молоді, а також для запобігання витоку конфіденційної інформації через загрози пов'язані з несанкціонованим доступом до даних користувачів.

Метою даної роботи є захист інформації у апаратно-технічних приміщеннях спорткомплексу «Минай».

Методами дослідження є пошук та захисту вразливих і слабких до витоку інформацій місць. Для досягнення мети необхідно виконати такі завдання: аналіз приміщень у спорткомплексі, опис і визначення контрольованої зони описати рівні захисту, визначити види витоку інформації та описати їх, захист об’єкту. Під час досліджень було розглянуто алгоритм захисту інформації у приміщені. Розписані по пунктах характеристики та класифікація витоків інформації. За складеним алгоритмом буде розроблятися комплексний захист апаратно-технічних приміщень спорткомплексі, для виконання поставлених задач по захисту інформації. Розглянуто схеми будівлі в якій розташовані приміщення для захисту від витоків інформації. Досліджено матеріали з яких зроблена будівля та приміщення. Розглянути декілька каналів витоку інформації та розписані розписали їх. Виходячи із отриманих даних, запропоновано методи та засоби для запобігання витоку інформації відповідно до їх каналів.

ЗАХИСТ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ У ФІЛІЇ МЕДИЧНОГО ЦЕНТРУ «ІНТЕРСОНО»

Пасіка Марк

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54,
студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

Істотна частина проблем забезпечення захисту інформації в комп'ютерній системі може бути вирішена організаційними заходами. Проте, з розвитком інформаційних технологій, спостерігається тенденція зростання потреби застосування технічних заходів і засобів захисту. Тому робота на тему «Захист інформації від несанкціонованого доступу у філії медичного центру «Інтерсоно» являється безперечно актуальною.

Метою дослідження являється мінімізації загроз витоку інформації у філії приватного медичного центру «Інтерсоно».

Клініки, медичні центри, інші установи охорони здоров'я стикаються з великою кількістю персональних даних як співробітників, так і клієнтів. Багато документів потрапляють в категорію лікарської таємниці [1]. Тому інформаційна безпека в медицині переходить на новий рівень.

Медичні заклади переходять на електронний документообіг, автоматизується ведення електронного обліку або медичних карт пацієнтів. З розвитком інформаційних технологій прискорився і перехід медичних установ на новий рівень обробки і зберігання персональних даних.

Одним з напрямків захисту інформації в інформаційних системах є технічний захист інформації. У свою чергу, питання технічного захисту інформації розбиваються на два великих класи завдань: захист інформації від несанкціонованого доступу і захисту інформації від витоку технічними каналами [2]. Під несанкціонованим доступом звичайно мається на увазі доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розглядаються канали сторонніх електромагнітних випромінювань і наведень, акустичні

канали, оптичні канали й ін.

Інформаційні ресурси які знаходяться у філії медичного центру «Інтерсоно» є цінними, мають відповідне матеріальне вираження і вимагають захисту від різноманітних за своєю сутністю впливів і загроз

Проведено аналіз і запропоновано комплекс заходів та методи вдосконалення комплексного захисту інформації для філії медичного центру «Інтерсоно».

1. Закон України Про захист персональних даних від 01.06.2010 № 2297-VI

2. Остапов С. Е. технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

ЗАХИСТ ІНФОРМАЦІЇ В СИСТАМАХ МОБІЛЬНОГО ЗВ'ЯЗКУ ТА НАПИСАННЯ ДОДАТКУ ДЛЯ ШИФРУВАННЯ ТЕКСТОВОЇ ІНФОРМАЦІЇ МЕТОДОМ RIJNDAEL

Бонкало Василь Анатолійович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54,
студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

Сьогодні досить актуальною є проблема безпеки інформації. У наш мобільний час важливе місце відводиться проблемі інформаційної безпеки та забезпечення конфіденційності даних. Для захисту інформації на рівні прикладного та системного ПЗ використовуються системи розмежування доступу до даних, системи ідентифікації та автентифікації, системи аудиту та моніторингу, а також системи антивірусного захисту. Основним методом шифрування інформації – є криптографічний. На сучасному етапі розвитку науки і техніки саме криптографія дає можливість здійснювати безпечний обмін інформацією.

В ході роботи, було проаналізовано методи та алгоритми шифрування в мобільному зв'язку, їх основні характеристики, переваги та недоліки. На основі аналізу написано додаток для шифрування текстової інформації методом Rijndael, та вдосконалено його з 128 бітного ключа на 256 бітний ключ з урахуванням всіх недоліків попередніх шифрувань.

Додаток було проаналізовано на криптостійкість, що дало чудовий результат, оскільки для несанкціонованого розшифрування інформації написаного з використанням методу Rijndael потрібно щонайменше пів століття в залежності від потужності комп'ютеру, який буде її розшифровувати, а з урахуванням того, що ключ змінюється не рідше 1 разу на тиждень, зловмиснику категорично буде обмаль часу для викрадення важливої інформації.

Дана програма може надійно захищати дані в мобільній мережі, та в подальшому суттєво підвищить популярність використання цього методу для захисту інформації.

ЕВОЛЮЦІЯ РАМАН СПЕКТРІВ СКЛОПОДІБНОГО C-GeS_2 ПРИ ТЕХНОЛОГІЧНОМУ МОДИФІКУВАННІ

Гевці Давид Олександрович

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

Зразки склоподібного c-GeS_2 синтезували шляхом гартування розплаву від різних температур - 1173 K (T_1) до 1373 K (T_3) та швидкостях гартування від 100 K/c (V_1) до 150 K/c (V_2). Далі чотири різні зразки c-GeS_2 будуть позначатися (T_1,V_1), (T_2,V_2), (T_3,V_1) і (T_3,V_2). Технологічно модифікований g-GeS_2(T_iV_j), досліджували за допомогою Раманівської спектроскопії. Зняті Раман-спектри показали, що інтенсивність смуг при 370 і 433 $см^{-1}$ в нормалізованих спектрах стекол залежить від умов одержання. Для стекол, отриманих гартуванням від більших температур розплаву, інтенсивність цих смуг зростає. При менших значеннях температури розплаву (T_1,V_1) в Раман спектрах також спостерігається подібний ефект. Найменша інтенсивність цих смуг була виявлена в Раман спектрах *c*-GeS_2, синтезованого при умовах (T_2,V_2). У цьому випадку не виявлені смуги в області 200-300 $см^{-1}$, але виявлено слабоінтенсивну смугу біля 490 $см^{-1}$, характерну для коливань S-S зв'язків. Значні зміни Раман спектрів *c*-GeS_2 при зміні умов синтезу були зафіксовані в області 200-300 $см^{-1}$. Так в мікро-Раман спектрі *c*-GeS_2, (T_3=1373 K) появляється інтенсивна смуга з максимумом при 256 $см^{-1}$.У випадку збудження Раман-сигналу з енергією фотонів 2.41 еВ, смуга при 256 $см^{-1}$ детектується навіть для зразка, синтезованого при умовах (T_1,V_1), в той же час в макро-Раман спектрах, збуджених при енергії фотонів 1.17 еВ, її зафіксовано не було. В мікро-Раман спектрі *c*-GeS_2(T_3,V_2) вже чітко проявляється структура піку 256 $см^{-1}$ з перегином при 237 $см^{-1}$. Положення основних цих смуг в області 200-300 $см^{-1}$ добре узгоджується як з положенням смуг в поляризованих Раман спектрах кристалу *к*-GeS (212, 240 і 272 $см^{-1}$), так і з частотним положенням Раман-

активних мод розрахованих для кластерів з потрійно координованою сіркою – $SGe_{3/3}$ і SGe_3-$S_{6/3}$. Резонанс коливних мод при 370 і 433 $см^{-1}$ відбувається для всіх стекол $GeS_2(T_i,V_j)$ при збудженні розсіювання з енергією фотонів 2.54 еВ. Положень та інтенсивності смуг при 370 і 433 $см^{-1}$ в спектрах КРС *c*-GeS_2 добре узгоджуються з розрахованими Раман-активними модами кластеру $Ge_2S_{2+4/2}$ де тетраедри GeS_4 зв’язані по ребру

ПРОЕКТУВАННЯ ЗАХИЩЕНОГО ОПТОВОЛОКОННОГО КАНАЛУ ЗВ'ЯЗКУ

Мачужак Богдан Олександрович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54,
студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

За останній етап розвитку в галузі зв'язку максимального поширення набули оптичні кабелі і волоконно-оптичні системи передачі, які за своїми характеристиками набагато перевершують всі традиційні кабелі системи зв'язку. Зв'язок по волоконно-оптичним кабелям, є одним з ключових напрямків науково-технічного прогресу. Кабелі та оптичні системи застосовуються не тільки для обчислювальної техніки, але ще й для організації телефонного міського, а так само міжміського зв'язку, кабельного телебачення, відеотелефонії, радіосповіщення, технологічного зв'язку і т.д.

У даний час з кожним днем все більше зростає кількість корпоративних мереж, існуючі мережі розширюються, зростає число користувачів цих мереж. Причому ростуть також і вимоги до інформаційних ситем. Головними напрямками соціального і економічного розвитку країни визначено програму подальшого розвитку зв'язку, яка передбачає продовжити розвиток і підвищити надійність зв'язку країни на базі новітніх досягнень науки і техніки та розвинути високоавтоматизоване виробництво волоконно-оптичних кабелів зв'язку.

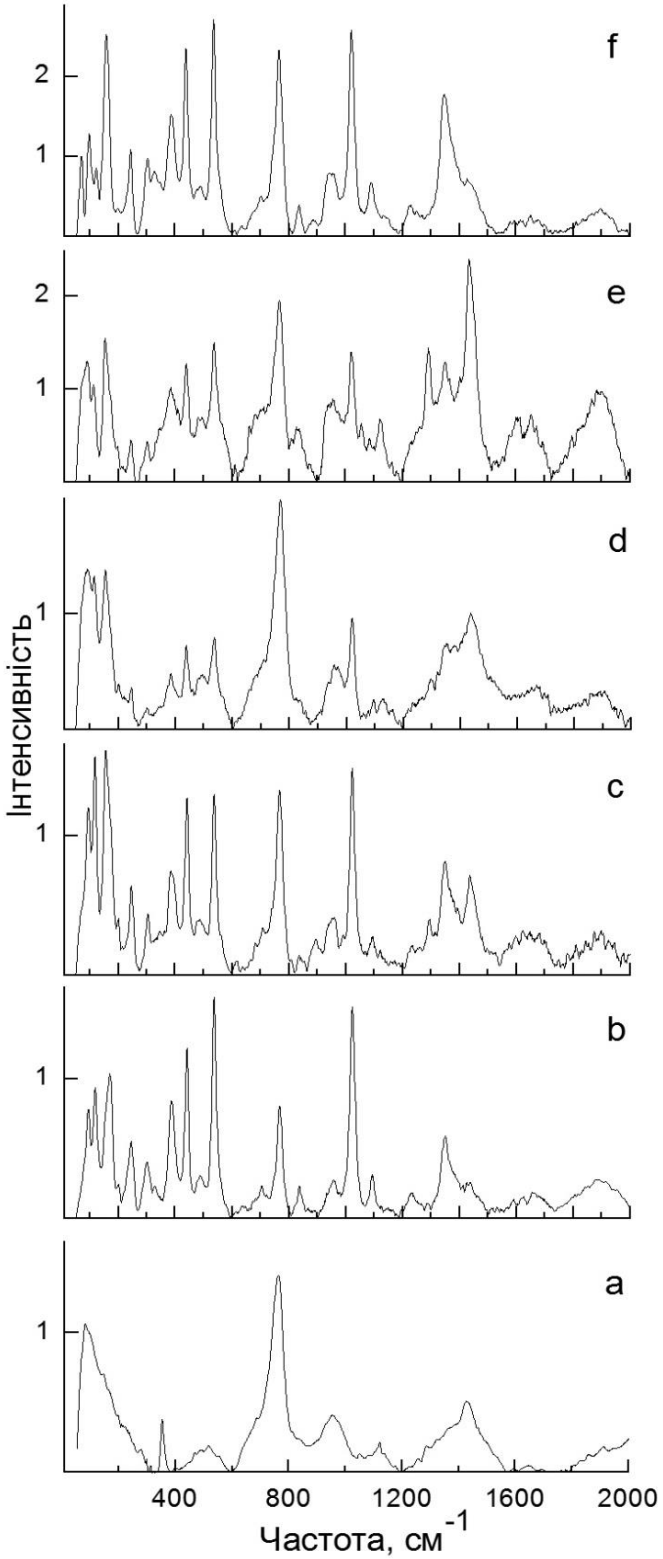
У даній роботі здійснено дослідження всіх відомих методів несанкціонованого доступу до оптоволоконних ліній, а також просто небажаних каналів витоку інформації через ці лінії. Також провівся аналіз методів забезпечення безпеки ВОЛЗ для застосування їх на практиці при проектуванні конкретної лінії зв'язку, що прокладатиметься від ПРАТ «Датагруп» до магазину електроніки «MOYO» .

КОМБІНАЦІЙНЕ РОЗСІЮВАННЯ СКЛОПОДІБНОГО $Li_2B_4O_7$, АКТИВОВАНОГО Tb_2O_3

Савчин Андрій Михайлович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54, фізичний факультет
студент магістратури 2 року навчання

Було виконано експериментальне вивчення ефектів домішкового розсіювання у спектрах КР склоподібного тетрабората літію, активованого іонами Tb_2O_3, оскільки рідкоземельні елементи (РЗЕ) входять у структуру твердих тіл у вигляді тризарядних іонів [1].



Спектри мікрораманівського розсіювання досліджували при температурі T=300 K у діапазоні 50–2000 $см^{-1}$ за допомогою лазерно-спектроскопічного комплексу Solar TII на базі дифракційного спектрометра MS7504 з системою реєстрації на базі CCD-камери HS101H. Використані для дослідження склоподібні зразки $Li_2B_4O_7$ (ТБЛ) були синтезовані за технологією, описаною в посиланні[2]. Концентрація активатора змінювалася у межах 5×10^{-4} — 5×10^{-2} ваг. % Tb_2O_3 (рис.) Для ідентифікації структури спектра КР склоподібного $Li_2B_4O_7$

було враховано особливості кристалохімічної будови тетрабората літію [3].

На підставі відомих частот коливань структурних комплексів [LiO_4], [LiO_3], [BO_4], [BO_3] проведено ідентифікацію однофононних спектрів склоподібного $Li_2B_4O_7$ (рис.). Різко виражена структура в діапазоні 77–400 $см^{-1}$ для скла ТБЛ відповідає нормальним коливанням каркасів [LiO_6]. У спектральній області 400–600 $см^{-1}$ має місце суперпозиція коливань каркасних груп [LiO_4] та тетраедрів [BO_4]. Максимуми в діапазоні частот 600–800 $см^{-1}$ зумовлені коливаннями комплексів [LiO_4]. За нормальні коливання цих же комплексів відповідають піки в спектральних інтервалах 800–1200 $см^{-1}$ і 1160–1354 $см^{-1}$. Моди в області широкого максимуму при 953,3 $см^{-1}$ зумовлені деформацією тетраедрів [BO_4], а за коливання при 352,5 $см^{-1}$ відповідає розтяг тетраедрів [BO_4]. Симетричному розтягу групи [BO_3] відповідають частоти 828,0 та 953,3 $см^{-1}$. Найбільш інтенсивна мода при 763 $см^{-1}$ характеризує коливання симетричних деформацій комплексів [BO_3](рис).

Показано, що при активуванні склоподібного тетрабората літію Tb_2O_3 структура спектрів КРС суттєво ускладнюється і для всіх зразків з різними конструкціями активатора подібна. Порівняння цих спектральних залежностей зі спектрами КРС монокристалічного ТБЛ, досліджених в поляризованому і не поляризованому світлі [1,3], показує на практично повне співпадання частот, коливальних мод в діапазоні 600-2000 $см^{-1}$, структура склоподібного $Li_2B_4O_7$ ймовірно залишається тригональною в межах усередненого порядку. При зміні концетрації іонів Tb^{3+} (рис.) спектр КРС $Li_2B_4O_7$: Tb^{3+} в частотній області 70-600 $см^{-1}$, співпадає з частотною залежністю КРС монокристалічного Tb_2O_3, що вказує на гібридизацію іонів Tb^{3+} в розупорядковану матрицю на місце іонів літію [4].

Досліджена динаміка зміни спектрів комбінаційного розсіювання світла склоподібного тетрабората літію, активованого оксидом тербію різної концентрації, підтверджує ефект гібридизації орбіти тризарядових іонів Tb^{3+} з матрицею $Li_2B_4O_7$, внаслідок чого структура склоподібного ТБЛ кластеризується і спостерігається часткове вклинення кубічної сингонії в тетрагональну. Встановлено, що більшість коливних мод, що спостерігалися в

досліджуваних спектрах, належать до змішаних коливань різних типів, які пов'язані деформованою каркасною будовою скла зі складних бор-оксидних та тербій- оксидних комплексів.

1. G.L. Paul, W. Taylor. Raman spectrum of $Li_2B_4O_7$ // J. Phys. C: Solid State Phys. – 1982. V.15. pp.1753–1764.

2. П.П. Пуга, Г.Д. Пуга, К.П. Попович, В.А. Кельман, В.Н.Красилинец, М.М. Турок, Н.В. Примак, П.С. Данилюк. Оптичиское поглощение ренгенолюминисценции склообразного тетрабората лития , активированого окидом тербия// Физика и химия стекла -2012.Т.38.№2.с.209-216.

3. R. Shuker, R.W. Gammon. Raman-scattering selection-rule breaking and the density of states in amorphous materials // Phys. Rev. Lett. – 1970. V.25. No.4. pp.222–225.

4. L.A.Tucker, F.J. Carney, P.McMillan, S.H.Lin,L.Eyring. Raman and resonance. Raman spectroscopy of selected rare-earth sesquioxides// Applied spectroscopy.-1984- v.38 №6 –pp.857-860.

ACCELERATE Satellite Session at the V Regional Scientific-Practical Conference "INFORMATION TECHNOLOGIES IN THE LIFE OF STUDENTS AND YOUNG SCIENTISTS OF TRANSCARPATHIA"

07 November 2019, aud.181 UzhNU, 54, Voloshina st., Uzhhorod (Ukraine)

Programme

Invited lectures:

Vladimir Matolin, Salma Baghdadi, Vasyl Rizak	"**CERIC-ERIC Outpost at the Department of Solid State Electronics and Information Security of Uzhgorod University**"
Vladimír Komanický	**"Electron-induced phenomena in chalcogenide films and their application to lithography"** Institute of Physics, Faculty of Science, Safarik University, Kosice, 04001, Slovakia
Viktor V. Bunda	"**Application of the "High Temperature Superconductors/ Photosemiconductors" Heterojunctions in Photonics"** Transcarpathian Academy of Arts, Voloshina St., 37, 88000 Uzhgorod, Ukraine

Mahdalyna Opachko	"**Designing of information and educational environment for studying physics at school by masters – futureteachers**"" Faculty of Social Sciences, Uzhhorod National University, Ukraine.
Mykhaylo Pahirya	"**Multiplatform tools for implementing cryptology algorithm**s" Mukachevo State University, Ukraine
Mykhaylo Povidaichyk, Dmytro Maiors′kyi, Dmytro Olashyn	"**Development of information system of semantic analysis of mathematical text**" Faculty of Mathematics, Uzhhorod National University, Ukraine.
Ihor Povkhan	"**The general concept of algorithmic classification tree in pattern recognition problems"** Faculty of Information Technologies, Uzhhorod National University, Ukraine.
Mykhailo Pryhara	'"**Using a geographic information system (GIS) in Planning and Management"** Faculty of Engineering, Uzhhorod National University, Ukraine.
Vasyl Rubish	'"**New type recording media based on nanostructured chalcogenide materials"** Institute for Information Recording of the National Academy of Sciences of Ukraine.

Invated lecture

ELECTRON-INDUCED PHENOMENA IN CHALCOGENIDE FILMS AND THEIR APPLICATION TO LITHOGRAPHY

Vladimír Komanický

Institute of Physics, Faculty of Science, Safarik University, Kosice, 04001, Slovakia

This paper presents our recent studies with the binary and ternary chalcogenide systems have revealed electron-induced effects. Investigations of the interaction of electron beam with chalcogenide films have shown formation of a surface reliefs of various types depending on the charge deposited in the film. When the electron beam hits the surface of the films takes formation of the surface relief. The kinetics of the formation of the surface relief, the change in its shape and parameters during electron irradiation of the chalcogenide films (Figure) can be explained using the charge model. The mechanism of the formation of various types of surface relief in this model is the electrostatic interaction in the space charge region caused by the formation of dynamically changing of two charged layers, which are induced in the chalcogenide film during its electron irradiation. The appearance of a surface relief of various shapes on an chalcogenide film under electron irradiation indicates the possibility of using this material as an electronic resist for a single-stage (without chemical etching) electron lithography. Such parameters of interaction of chalcogenide films with an electron beam were calculated for the process of electron lithography: the penetration depth of electrons into chalcogenide film, the depth of the exit of secondary and reflected electrons, the accumulated charge, and the inversion dose. Using DrawBeam

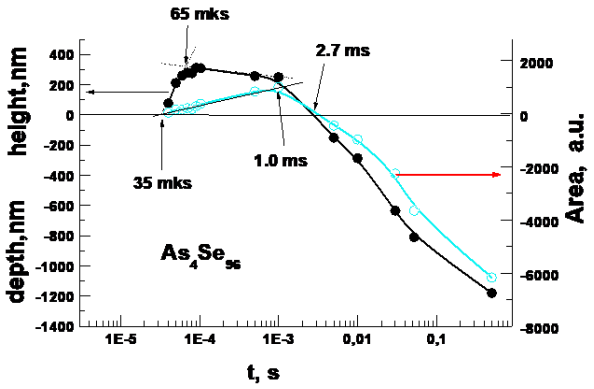


Fig. Changes of the parameters of the electron-induced surface relief of As_4Se_{96} film depending on the irradiation time: height — the height of the cones, depth — the depth of the craters, area — the axial section area.

software module included in the SEM software, standard images were taken by the negative and a positive electron lithography method on the chalcogenide films. Also, images of some of the logos on this film were made, which can be used to create hologram elements.

Invated lecture

ПІДГОТОВКА МАГІСТРІВ – МАЙБУТНІХ УЧИТЕЛІВ ДО ПРОЕКТУВАННЯ ІНФОРМАЦІЙНО-ОСВІТНЬОГО СЕРЕДОВИЩА ДЛЯ ВИВЧЕННЯ ФІЗИКИ В ШКОЛІ

Магдалина Опачко

доктор пед. н., доцент, професор каф. загальної педагогіки та педагогіки вищої школи ДВНЗ «УжНУ»

Аналіз навчальної, монографічної, періодичної літератури, дисертаційних фондів та електронних джерел інформації свідчить, що ефективність використання інформаційно-комунікативних технологій (ІКТ) у школі як засобу підвищення мотивації школярів в навчанні, розвитку їхніх творчих здібностей і пізнавальної самостійності, розвитку логічного мислення, формування інформаційної культури – є доведеним фактом. Таким чином, необхідною професійно орієнтованою складовою результатів навчання майбутніх учителів фізики є їх підготовка до застосування інформаційних технологій у процесі вивчення фізики у сучасній школі.

Застосування комп'ютера на уроках фізики як засобу навчання потребує розв'язання цілої низки проблем: визначення місця ІКТ в навчально-виховному процесі; вибір електронних засобів навчального призначення (ЕЗНП) та їх поєднання з традиційними для навчання фізики засобами; організація навчально-пізнавальної діяльності учнів на уроці, на якому застосовуються ІКТ.

Зазначене вище дозволяє сформулювати вимоги до вчителя фізики, який, в свою чергу, повинен: володіти основами використання, поняттями (термінологією), засобами, програмами та методами ІКТ; сприймати ІКТ як складову професійної діяльності; знати цілі використання ІКТ в змісті викладання фізики як навчальної дисципліни; використовувати ІКТ в якості дидактичного посередника, відповідно до цілей та етапів навчання (використання ІКТ в якості допоміжного засобу в організації фізичного

експерименту, використання ІКТ як «дидактичного супроводу» у реалізації цілей і завдань проблемної, розвивальної, ігрової, контекстної, діяльнісної, особистісної, задачної технологій навчання тощо); планувати й проектувати навчальну діяльність у сучасному навчальному середовищі, забезпечувати діагностику рівнів навчальних досягнень учнів.

Варто також згадати про можливості використання ІКТ у позашкільній освіті, зокрема, у гуртковій роботі. Все це обумовлює відповідні вимоги до підготовки майбутніх учителів. Сутність цих вимог полягає у формуванні здатності у майбутніх педагогів проектувати інформаційно-освітнє середовище для вивчення фізики в школі.

У змісті підготовки майбутнього вчителя фізики до проектувати інформаційно-освітнього середовища варто враховувати: тенденції інформатизації суспільства та освіти, зокрема розвитку інформаційно-комунікаційних технологій навчання; специфіку навчання природничих дисциплін, зокрема фізики та її відображення у електронних засобах навчання, які є об’єктами вивчення та засобами навчання; опору у підготовці вчителя на комплексний підхід як збалансоване поєднання контекстного, особистісно-діяльнісного, праксеологічного, компетентнісного та культурологічного підходів) тощо.

Організація навчання діяльності проектування ґрунтується на знаннях з інформатики, методики навчання фізики в школі і реалізується у змісті курсу «Основи педагогічної майстерності». Сутність навчання проектуванню полягає у роботі над проектом «Створення ІКТ-комплексу вивчення розділу (*назва розділу співпадає з назвою опорної теми*)». Опорна тема з фізики – це система наукових знань з певного розділу шкільного курсу фізики, яку студенти обирають за власним уподобанням.

У процесі роботи над проектом здійснюється систематизація знань студентів про можливості і обмеження використання комп’ютерних технологій у процесі вивчення фізики в школі. Системне опрацювання основних завдань проекту забезпечується виокремленням етапів: ознайомчого (знайомство із наявним та доступним ліцензованим програмним забезпеченням, створеним для

навчання фізики), аналітичного (аналіз програмних продуктів у контексті цільового призначення, змістового наповнення, можливості для використання тощо), творчого (добір ІКТ-моделей для навчання у розрізі опорної теми, розробка власних ІКТ-проектів), результативного (створення ІКТ-комплексу для опорної теми).

Для досягнення цілей проекту студентам пропонується виконати завдання:1) Проаналізувати доступну і наявну програмно-методичну базу для навчання фізики: CD-диски мультимедійних курсів фізики «Відкрита фізика», «Бібліотека електронної наочності», «Фізична віртуальна лабораторія», «Фізика 7кл.», «Фізика 8кл.», «Фізика 9кл.» , «Фізика 10кл.», «Фізика 11кл.»; CD-диски електронних енциклопедій. Створити електронний каталог відеоматеріалів для вивчення опорної теми. 2) Проаналізувати презентації у контексті опорної теми, що пропонуються для навчання фізики в Інтернет-мережі за критеріями: а) цільове призначення та цільова адекватність представленої інформації; б) обсяг інформації; в) визначеність місця і ролі презентації у вивченні теми (у змісті уроку) г) спрямованість представленої інформації: на розширення знань і уявлень; на створення чогось, або проведення експерименту; на «наочність заради наочності»; загальне враження від перегляду (як подано слайди з таблицями, малюнками і відео кліпами, графіками і діаграмами; як використовується кольорова гама та анімація тощо). 3) Проаналізувати можливості використання ІКТ в контексті реалізації компонент опорної теми в процесі навчання: актуалізація опорних понять; засвоєння нових понять; формування експериментальних та практичних умінь і навичок, діагностиці рівнів засвоєння знань, узагальнення і систематизації. 4) Узагальнити опрацьовані матеріали і представити створений ІКТ-комплекс для вивчення опорної теми у формі публічної презентації.

Перспективи подальших досліджень пов’язані із визначенням критеріїв оцінки рівнів готовності магістрів до проектування інформаційно-освітнього середовища для вивчення фізики в школі.

РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ СЕМАНТИЧНОГО АНАЛІЗУ МАТЕМАТИЧНОГО ТЕКСТУ

Михайло Повідайчик, Дмитро Майорський, Дмитро Олашин

ДВНЗ «УжНУ», Математичний факультет

Розглядається задача автоматизованого формування математичних виразів на основі семантичного аналізу тексту. Опишемо утиліту на мові VBA для текстового процесора MS Word, яка, використовуючи базу знань на мові Visual Prolog, за допомогою об'єкта OMath генерує деякі математичні вирази, описані природною мовою.

Лістинг 1. Утиліта «Текст_Формула».

```
Sub Текст_Формула()
  Dim a As OMath
  Dim s$, p%
  s = Trim(Selection.Range.Text)
  If Len(s) > 0 Then
    Selection.OMaths.Add Range:=Selection.Range
    Set a = Selection.OMaths(1)
    Open "Формула.txt" For Output As #1
    Print #1, "текст(" & Chr(34) & s & Chr(34) & ")"
    Close #1
    Shell ThisDocument.Path & "\" & "Goal.exe"
    MsgBox "Працює макрос ..."
    Open "d:\Формула.txt" For Input As #1
    Line Input #1, s
    Close #1
    s = Mid(s, 8)
    s = Mid(s, 1, Len(s) - 2)
```

```
    a.Range.Text = s
    a.BuildUp
  End If
End Sub
```

Приведена програма передає математичний текст, описаний природною мовою, у середовище Visual Prolog, де реалізовані правила його опрацювання і перетворення у «лінійний» вигляд. Використовуючи метод BuildUp об’єкта OMath, вираз представляється у «професіональному» виді.

Далі будуть розглядатися задачі розпізнавання фрагменту тексту, який містить описання математичного виразу, розробки автоматизованої системи налаштування «під користувача», побудови графічних об’єктів та ін.

Invated lecture

ЗАГАЛЬНА КОНЦЕПЦІЯ АЛГОРИТМІЧНОГО ДЕРЕВА КЛАСИФІКАЦІЇ В ЗАДАЧАХ РОЗПІЗНАВАННЯ ОБРАЗІВ

ПОВХАН ІГОР ФЕДОРОВИЧ

ДВНЗ "Ужгородський національний університет",
факультет інформаційних технологій,
кафедра програмного забезпечення систем

Аналізуючи проблематику деревоподібних моделей класифікації та розпізнавання можна побачити певний брак поточних досліджень в цьому напрямку, коли головна увага зміщена в бік концепції нейромережевого розпізнавання. В значній мірі це пояснюється особливостями самих моделей логічних дерев класифікації (ЛДК), складнощами реалізаційних моментів концепції алгоритмічного дерева класифікації (АДК) (найвищого рівня абстракції концепції ЛДК), набором жорстких правил та обмежень щодо практичної роботи з такими структурами даних [1-3]. Тим не меньше, представлення навчальних вибірок (дискретної інформації) великого об'єму у вигляді структур логічних дерев має свої суттєві переваги в плані економічного опису даних та ефективних механізмів роботи з ними [4]. Тобто – покриття навчальної вибірки набором елементарних ознак у випадку ЛДК, або покриття навчальної вибірки фіксованим набором автономних алгоритмів розпізнавання та класифікації у випадку АДК, породжує фіксовану деревоподібну структуру даних, яка в якісь мірі забезпечує навіть стиск та перетворення початкових даних НВ – а отже дозволяє суттєву оптимізацію та економію апаратних ресурсів системи. Відмітимо, що галузь застосування концепції ЛДК зводиться до задач опису структур даних, задач розпізнання та класифікації, задач регресії [5].

Так як головну ідею методів та алгоритмів ЛДК можна визначити як оптимальну апроксимацію деякої початкової НВ набором елементарних ознак

(атрибутів об‘єкту), то на перший план виходить їх центральна проблема – питання вибору ефективного критерію розгалуження (відбору вершин, атрибутів, ознак дискретних об‘єктів). Саме цим принциповим задачам присвячені роботи [5-8] де піднімаються питання якісної оцінки окремих дискретних ознак, їх наборів та фіксованих сполучень, що дозволяє запровадити ефективний механізм реалізації розгалуження.

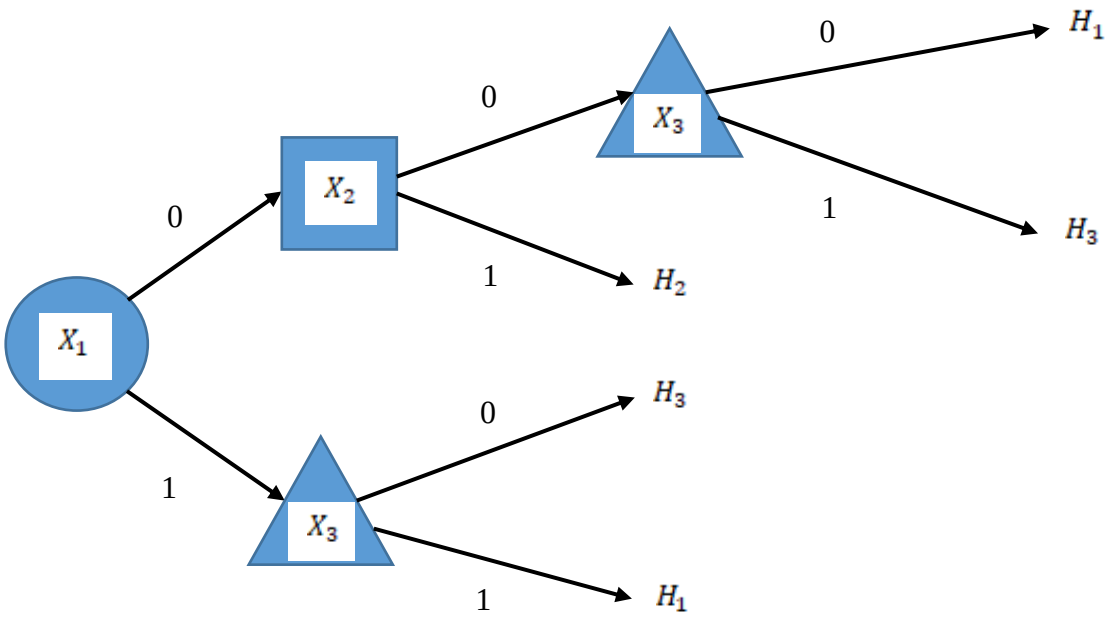


Рис. 1 Загальна схема ЛДК побудованого за алгоритмом з покроковою оцінкою важливості ознак.

Приклад АДК яке побудоване за даними НВ на основі методу розгалуженого вибору ознак зображено на (Рис. 1) (алгоритм з покроковою оцінкою важливості ознак). Зауважимо, що дане дерево не є регулярним і на різних ярусах розташовані різні мітки в залежності від їх оцінки інформативності на кожному кроці. Так на першому кроці з найбільшою інформативністю обирається атрибут x_1, на другому x_2, на третьому x_3, на четвертому знову x_3 (послідовність – зліва на право, зверху в низ). Причому на кожному кроці відбувається фактичне розбиття початкової НВ на підмножини з наступним етапом відбору найбільш якісної, інформативної ознаки (генерації

вершини), а загальна схема побудови ЛДК актуальна не тільки для бінарного випадку атрибутів [7].

Звернемо увагу, що концепції логічних дерев не протирічить можливість в якості ознак (вершин) ЛДК використовувати не тільки окремі атрибути (ознаки) об‘єктів їх сполучення (ідея узагальненої ознаки, розглядалась в роботі [4]) та набори, але якщо піти далі та не розглядати в якості розгалужень атрибути об‘єктів (ознаки) – а відбирати окремі незалежні алгоритми розпізнавання (оцінені за даними НВ) то на виході буде отримане нова структура – АДК.

[1]. Quinlan J.R. Induction of Decision Trees // Machine Learning. 2008, № 1, P. 1−81. 22.

[2]. Василенко Ю.А., Повхан І.Ф., Ващук Ф.Г. Проблема оцінки складності логічних дерев розпізнавання та загальний метод їх оптимізації // Науково технічний журнал “European Journal of Enterprise Technologies”. 2011, 6/4(54), С. 24-28.

[3]. Повхан І.Ф., Василенко Ю.А., Василенко Е.Ю. Концептуальна основа систем розпізнавання образів на основі метода розгалуженого вибору ознак // Науково технічний журнал “European Journal of Enterprise Technologies”. 2004, №7[1], С. 13-15.

[4]. Povhan I. Designing of recognition system of discrete objects // IEEE First International Conference on Data Stream Mining & Processing (DSMP), Lviv - 2016, Ukraine, P. 226-231.

[5]. Povhan I. General scheme for constructing the most complex logical tree of classification in pattern recognition discrete objects // Збірник наукових праць "Електроніка та інформаційні технології", Львів. 2019, Випуск 11, С. 112-117.

[6]. Vasilenko E. Yu., Kuhayivsky A., I., Papp I. O., Vasilenko Yu. Construction and optimization of recongnizing systems // Науково технічний журнал “Інформаційні технології і системи”, Львів 1999, № 1(Т1), С. 122-125.

[7]. Повхан І.Ф., Василенко Ю.А. Групова та індивідуальна оцінка важливості бульових аргументів // Вісник національного технічного університету «ХПІ». 2011, №53, С. 57-64.

[8]. Повхан І.Ф. Проблема функціональної оцінки навчальної вибірки в задачах розпізнавання дискретних об‘єктів // Вчені записки Таврійського національного університету. Серія: технічні науки. 2018, Том 29 (68) № 6 2018, С. 217-222.

Invated lecture

GROWN, CRYSTAL STRUCTURE AND MECHANISM OF PHOTOCONDUCTIVITY OF BiOCl SINGLE CRYSTALS

V.Bunda[1], S, Bunda[1], A. Feher[2]

[1] Transcarpathian Academy of Arts, Voloshina St. 37, Uzhgorod 88000, Ukraine

[2] Centre of Low Temperature Physics, Faculty of Science P. J. Šafárik University & Institute of Experimental Physics, Slovak Academy of Sciences, Park Angelinum 9, Kosice 04154, Slovakia

In recent years, two-dimensional (2D) materials, such as single crystals, nanoplates and nanosheets, have attracted much attention because of not only their unique electronic, magnetic, optical, and catalytic properties, which mainly arise from their large surface areas, nearly perfect crystallinity, structural anisotropy, and quantum confinement effects in the thickness

Oxyhalides of bismuth BiOX (X = Cl, Br, I) are very interesting materials which find various applications as X-ray luminescent screens, as anti-Stokes converters, photocatalyst, usual luminophors and as photoconductive analyzer of linear polarized radiation in the 0.24 - 1.2μ spectral region. The great interest for these materials is strongly related to the influence of dimensionality on the behaviour of physical properties (they are 2D structured materials). Bismuth oxyhalides are one of the V-VI-VII group compound semiconductors belonging to the tetragonal system. The structure of BiOX is known to have a layered structure, which is constructed by the combination of the halide ion layer and the bismuth oxygen layer. We present results of the study of BiOCl single crystals photoconducting spectra.