МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут комп`ютерних систем і технологій
"Індустрія 4.0" ім. П.М. Платонова
Факультет Комп`ютерної інженерії, програмування та кіберзахисту

XX Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції. Частина І.

Одеса

21-22 квітня 2020 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XX Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Частина І. Одеса, 21-22 квітня 2020 р. - Одеса, Видавництво ОНАХТ, 2020 р. - 240 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані по секціях кафедри інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова - д.т.н., проф., **Єгоров Б.В.**, ректор ОНАХТ.

Співголови:

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи ОНАХТ,
Котлик С.В. – к.т.н., доц., директор ННІКСіТ "Індустрія 4.0" ОНАХТ,
Даріуш Долива, д.математичн.наук, уповноважений декана факультету Інформатики УІтаПЗ, м. Лодзь, Польща,
Ковалюк Т.В. - к.т.н., доц. кафедри АСОІтаУ НТУУ «Київський політехнічний інститут».

Члени оргкомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри ІТтаКБ ОНАХТ,
Артеменко С.В. – д.т.н., проф., завідувач кафедри КІ ОНАХТ,
Князєва Н.О. – д.т.н., проф. кафедри КІ ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри АТПтаРС ОНАХТ,
Тарасенко В.П. – д.т.н., проф., завідувач кафедри СКС НТУУ «Київський політехнічний інститут»,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри КІТАМ ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ "Львівська політехніка",
Жуков І. А. – д.т.н., проф., завідувач кафедри КСтаМ НАУ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

СЕКЦІЯ № 1

Комп'ютерні науки

Тематичні напрями:

МАТЕМАТИЧНЕ І КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ СКЛАДНИХ ПРОЦЕСІВ

УПРАВЛІННЯ, ОБРОБКА ТА ЗАХИСТ ІНФОРМАЦІЇ

НОВІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

ПРОЕКТУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ПРОГРАМНИХ КОМПЛЕКСІВ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА КІБЕРБЕЗПЕКИ

ОДЕСЬКОЇ НАЦІОНАЛЬНОЇ АКАДЕМІЇ ХАРЧОВИХ ТЕХНОЛОГІЙ

Список
скорочень організацій, представники яких взяли участь у конференції

Таблиця 1

Скорочення	Повна назва організації
АУПРБ	Академия управления при Президенте Республики Беларусь
БГЄУ	Белорусский государственный экономический университет
ВНТУ	Вінницький національний технічний університет
ДДПУ	ДВНЗ «Донбаський державний педагогічний університет»
УДХТУ	ДВНЗ «Український державний хіміко-технологічний університет»
ДДТУ	Дніпровський державний технічний університет
ДДМА	Донбаська державна машинобудівна академія
ДНТУ	Донецький національний технічний університет
ДНУ	Донецький національний університет ім. Василя Стуса
ІФНТУНГ	Івано-Франківський національний технічний університет нафти і газу
ІІТЗН	Інститут інформаційних технологій і засобів навчання НАПН України
ІТТНАН	Інститут технічної теплофізики НАН України
КНУ	Київський національний університет імені Тараса Шевченка
НТУУ "КПІ"	Національний технічний університет «Київський політехнічний інститут»
КПАІТ	Коледж промислової автоматики та інформаційних технологій ОНАХТ
КДПУ	Криворізький державний педагогічний університет
НУ"ПП"	Національний університет «Полтавська політехніка імені Юрія Кондратюка»
НТУ «ХПІ»	Национальный технический университет "Харьковский политехнический институт"
ОНПУ	Одеський національний педагогічний університет ім.Ушінского
ОНАХТ	Одеська національна академія харчових технологій
ОНПУ	Одеський національний політехнічний університет
ОНУ	Одеський національний університет імені І. І. Мечникова
ПДАТУ	Подільський державний аграрно-технічний університет
РДГУ	Рівненський державний гуманітарний університет
СКХП	Сумський коледж харчової промисловості НУХТ
ТЛіАЛ	Технічний ліцей імені Анатолія Лигуна, Національний технічний університет «Дніпровська політехніка»
УАД	Українська академія друкарства
УДПУ	Уманський державний педагогічний університет імені Павла Тичини
ХНУ	Хмельницький Національний Університет
ХНУРЕ	Харківський національний університет радіоелектроніки
ЦУНТУ	Центральноукраїнський національний технічний університет
ЧНУ	Чорноморський національний університет ім. Петра Могили
IAE	Institute of Automation and Electrometry of the Siberian Branch Russian Academy
VNTU	Vinnytsia National Technical University

даних лабораторії. Вихідними даними блоку планування є вхідні дані для апаратної частини (датчики, автоматика синтетичного обладнання) та програмної підсистеми блоку хімічного синтезу – аналіз даних датчиків та керуючі сигнали для припинення існуючого або запуску наступного етапу синтезу.

Після синтезу продукт переходить до блоків характеризації та дослідження функціональних властивостей. Ці блоки є окремими і в них входить дослідницьке обладнання лабораторії або зовнішніх установ. У більшості обладнання цього блоку є автоматизованим, тому головним в цьому блоці є створення єдиної бази даних, формування потоків даних з багатьох приладів, управління їми при внесенні даних у єдину базу даних.

Таким чином, у роботі проаналізована структура, визначено робочі блоки та розподіл робочих потоків в лабораторії наноматеріалів ДонФТІ НАН України. Подальша робота буде спрямована на більш детальну декомпозицію усіх визначених блоків.

Список використанних джерел

1. Frey J.G. Dark Lab or Smart Lab: The Challenges for 21st Century Laboratory Software. //Org. Proc. Res. Dev.- №8.-2004. - P. 1024-1035.
2. Čolaković A., Hadžialić M. Internet of Things (IoT): A review of enabling technologies, challenges//Computer Networks. – 144. -2018. – P. 17-39.
3. I. Danilenko, O. Gorban, P. Maksimchuk,et all. Photocatalytic activity of ZnO nanopowders: The role of production techniques in the formation of structural defects// Catalysis Today. - 328. – 2018. - P.99-104, 2019

АНАЛІЗ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОНОГО ДОКУМЕНТООБІГУ

Грик Юрій Володмирович, аспірант:
Науковий керівник: Сельменська Зоряна Михайлівна, к.т.н., доцент
«Українська академія друкарства», м. Львів, Україна

Сьогодні існує велика кількість методів і технологій захисту інформації, призначених забезпечити конфіденційність, цілісність і доступність інформації. У роботі проаналізовано сучасні методи і технології захисту інформації в системах електронного документообігу (СЕД). Аналіз спрямований на полегшення організації системи комплексного та ефективного захисту інформації під час використання СЕД.

Ключові слова: СЕД, захист інформації, шифрування даних.

Мета статті - проаналізувати й узагальнити інформацію про наявні сьогодні засоби, методи підходи та технології захисту інформації в СЕД.

Стрімкий розвиток інформаційних технологій, широке розповсюдження мережі Internet і постійне зростання вартості інформації зумовлюють той факт, що захист даних у СЕД на сьогодні є однією з найважливіших проблем у сфері інформаційних технологій.

Згідно із Законом [1], захист інформації в інформаційній системі повинен здійснюватись шляхом створення комплексної системи захисту інформації з використанням засобів захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/ або криптографічного захисту інформації. Закон визначає два напрями, у яких повинен здійснюватись захист інформації: технічний і криптографічний.

Регулярне застосування засобів і методів захисту інформації допомагає забезпечити необхідну надійність інформації, що зберігається та обробляється з використанням засобів системи ЕД [2; 3].

Виходячи зі структури СЕД, до об'єктів захисту в СЕД можна віднести: робочі станції користувачів системи; робочі станції адміністраторів (мережі, бази даних, системи захисту тощо); сервери (мережеві, баз даних, додатків); апаратуру зв'язку (модеми, маршрутизатори); канали зв'язку (виділені або комутовані);

Найпоширенішими шляхами витоку інформації із СЕД, як і з будь-якої інформаційної системи, є: викрадення носіїв інформації та документів, які є результатом роботи системи; копіювання інформації на ПК; несанкціоноване підключення до апаратури та ліній зв'язку; перехоплення електромагнітного випромінювання в процесі обробки інформації.

Запобігання витоку інформації із системи переліченими вище шляхами здійснюється як технічними, так і криптографічними методами захисту інформації.

В асиметричних криптографічних системах для шифрування й дешифрування використовуються різні ключі. Ключ шифрування є відкритим, а таємність ключа дешифрування зберігається. При цьому відкритий ключ шифрування складений так, що він не дає змоги вирахувати секретний ключ дешифрування. Математичний взаємозв'язок між закритим і відкритим ключами робить кожну пару ключів унікальною.

Принципи асиметричної криптографії покладено в основу механізму захисту документів з використанням електронного цифрового підпису (ЕЦП), який набуває все більшого розповсюдження в СЕД. У таких системах також використовуються закритий і відкритий ключ ЕЦП. Відкритий ключ відомий усім користувачам системи й призначений для перевірки ЕЦП. Він допомагає визначити автора підпису та достовірність електронного документа, не даючи змоги обчислити секретний ключ.

Застосування криптографічних методів захисту інформації допомагає захищати безпосередньо інформацію, а не дає доступ до неї. Завдячуючи цим методам зберігаються дані, безпосередньо, в першоджерелі СЕД - в базі даних, сховищі, на сервері.

Цифрова стеганографія базується на приховуванні або вбудовуванні додаткової інформації в цифрові (як правило, мультимедійні) об'єкти, викликаючи при цьому певні їх спотворення без утрати функціональності. Методи стеганографії допомагають замінити несуттєві частки даних на конфіденційну інформацію, оскільки, можливості людини розрізняти дрібні зміни кольору або звуку обмежені. Стеганографія, зазвичай, використовується спільно з методами криптографії, доповнюючи її.

Новітнім і перспективнішим напрямом у технологіях захисту інформації є поєднання USB-брелків або смарт-карток та спеціального програмного забезпечення, призначеного для шифрування даних. Така технологія одержала назву Secret Disk. Вона базується на принципі шифрування даних на жорсткому диску. При цьому доступ до них можна отримати тільки за допомогою допоміжного ключа, який зберігається на зовнішньому пристрої. Перевага такого рішення полягає в тому, що захист даних забезпечується за допомогою алгоритму переміщення даних, а для того, щоб отримати доступ до зашифрованих даних, потрібні спеціальний пристрій (USB-брелок або смарт-картка) і введений із клавіатури пароль.

Принцип захисту даних за допомогою системи Secret Disk полягає в створенні на комп'ютері користувача (або сервері компанії) захищеного ресурсу - секретного диску, призначеного для безпечного зберігання конфіденційної інформації. У разі збереження, дані в захищених ресурсах шифруються. Доступ до цієї інформації та її розшифровка здійснюються, тільки, після приєднання до USB-порту комп'ютера електронного ключа.

Проаналізувавши відомі можливі способи захисту та приховування інформації в СЕД, можна резюмувати, що лише комплексне застосування усіх відомих, на теперішній час, організаційних, апаратних і програмних засобів у змозі забезпечити необхідний рівень таємності інформації.

Список використаних джерел

1. Про інформацію: Закон України. Відомості ВРУ (ВВР). 2005.№26 С.347.
2. Нішанбаєв Т., Рахімов Ф. Основи системного захисту даних в розподілених інформаційних системах URL: http://infocom.uz/2005/04/11/osnovyi-sistemnoy-zaschityi-dannyih-v-raspredelennyih-informatsionnyih-sistemah/
3. Захист інформації в процесі зберігання. URL: http://www.securit.ru/solution/store/.

XX Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

ОДЕСА
21-22 квітня 2020 р.

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Артеменко С.В., Ольшевська О.В.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.