

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 I.



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 I. 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
БГСУ	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
ІТЗН	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"ПІП"	Національний університет «Полтавська політехніка імені Юрія Кондратюка»
НТУ «ХПІ»	Национальный технический университет "Харьковский политехнический институт"
ОНПУ	Одеський національний педагогічний університет ім.Ушинського
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	Vinnitsia National Technical University

Іваненко М.М., Помпенко І.Г. Розробка графічного інтерфейсу для візуалізації функцій WEB-додатку для автоматизації роботи банкет-холу (КПАІТ, Україна)	86
Льящук Г.К., Приложенко В.Д., Антонова А.Р. Технології розробки мобільних додатків (ОНАХТ, Україна)	88
Іоргачов Є.Ю, Ломовцев П.Б. Дослідження безпеки зберігання даних у хмарному сховищі (ОНАХТ, Україна)	90
Капішевський Д.В., Помпенко І.Г. Розробка системи для автоматизацій управління проектами (КПАІТ, Україна)	91
Кіряк А.О. , Перова І.Г. Визначення найбільш інформативних питань тесту професійного вигорання за допомогою моделі логістичної регресії (ХНУРЕ, Україна)	93
Козін Д.О., Семенов А.О. Покращення характеристик смуго-стримуального фільтру за рахунок елементів із від'ємною диференційною ємністю (ВНТУ, Україна)	95
Комлева Г.О. Особливості проектування мережевого аукціону з використанням розвинутої системи чатів (ОНПУ, Україна)	97
Комлева О.О. Проектування програмного забезпечення відкритого наукового порталу (ОНПУ, Україна)	100
Королевич Є.М., Ольшевська О.В., Бодюл О.С. Розробка аналітичного інструментарію для побудови звітної документації (ОНАХТ, Україна)	102
Косухіна О.С., Москальова Т.В., Маньковська О. Моделювання та дослідження впливу конструктивних параметрів рами велосипеда на його ергономічні властивості (ДДТУ, ТЛіАЛ, Україна)	103
Котелевець І.О., Становська Т.П. Чат бот для комунікації салону краси NAILER (ОНАХТ, Україна)	105
Котлик Д.В., Мунтян І.В. Система управління 3d принтера Smartprint НВ-8, для створення 3D моделей будь-якої складності (КПАІТ, Україна)	106
Krachilova V., Mazurok I. Algorithmically expedient coding of the combinatorial problems solution (ONU, ONAFT, Ukraine)	108
Kurasov O.I., Liutenko I.V. Development of web service for assessment of software testing quality (NTU "KhPI", Ukraine)	110
Лаврєнов В.А., Зіменко Л.М. Аналіз та проектування веб-застосунку для публікації статей та нотаток (ОНАХТ, Україна)	112
Левитський Ю.О., Селіванова А.В. Засоби програмної підтримки підбору раціону дієтичного харчування (ОНАХТ, Україна)	114
Логвінов Д.О., Торяник Л.О. Розробка веб-сайту та телеграм-боту для зоомагазину (СКХП, Україна)	116
Майданюк В.П., Чернишов К.А. Ущільнення, завадостійке кодування та криптографія при захисті програм (ВНТУ, Україна)	117

- 1) пошук необхідних товарів у магазині за допомогою глобальної мережі Internet;
- 2) купівля та продаж товарів в умовах відсутності доступу до самого магазину, або у разі необхідності віддаленого здійснення операцій купівлі/продажу;
- 3) обмін відгуками із іншими користувачами та продавцем за допомогою веб-сайту та Telegram боту.

Список використаних джерел:

1. Luciano Ramalho, *Fluent Python: clear, concise, and effective programming*, 2015
2. Jay A. Kreibich, *Using SQLite*, 2010
3. Julia Elman & Mark Lavin, *Lightweight Django: using REST, websockets & backbone*, 2015
4. Django documentation // The Django software foundation: [Веб-сайт]. 2019. URL: <https://docs.djangoproject.com/en/3.0/>

**УЩІЛЬНЕННЯ, ЗАВАДОСТІЙКЕ КОДУВАННЯ ТА КРИПТОГРАФІЯ
ПРИ ЗАХИСТІ ПРОГРАМ**

**Майданюк В.П., к.т.н, доцент, Чернишов К.А., аспірант
Вінницький національний технічний університет**

Розрізняють захист програм:

- від випадкових загроз;
- захист від несанкціонованого доступу.

При захисті від випадкових загроз основними методами захисту є:

- дублювання інформації;
- використання завадостійких кодів – кодів, що виявляють помилки і кодів, що виявляють і виправляють помилки (корегуючі коди).
- методи формування контрольних сум, зокрема, з використанням циклічних завадостійких кодів;

Захист від несанкціонованого доступу забезпечують:

- криптографічні методи в першу чергу;
- методи формування контрольних сум, зокрема, з використанням циклічних завадостійких кодів;
- методи ущільнення даних (програми-пакувальники);
- програмно-апаратні методи (usb-ключі) та інші.

Використання методів криптографії та ущільнення даних при захисті програм від несанкціонованого доступу робить актуальним питання суміщення цих операцій.

У роботі К.Шеннона «Теорія зв'язку в секретних системах» (1949р.) було показано, що для деякого випадкового шифру кількість знаків шифротексту, отримавши який криптоаналітик при необхідних обчислювальних ресурсах зможе відновити ключ (тобто розкрити шифр), становить:

$$n = \frac{H(Z)}{r \log N}$$

де $H(Z)$ – ентропія ключа, r – надлишковість відкритого тексту, N -обсяг алфавіту. З виразу видно, що зниження надлишковості (ущільнення даних) може значно збільшити криптостійкість навіть для коротких ключів.

Донедавна алгоритми ущільнення даних і криптографічного захисту розвивались окремо, що призводило до значних обчислювальних витрат, оскільки при передачі і зберіганні файлів виникає необхідність в подвійному перетворенні інформації - спочатку ущільнення, а потім шифрування ущільненого файлу. Тому актуально є розробка таких алгоритмів шифрування даних, які б за один прохід виконували шифрування інформації з її одночасним ущільненням[1,2].

Головним критерієм при виборі алгоритму ущільнення для шифрування даних є мінімум затрат на адаптацію його до розв'язування нових задач. С цієї точки зору заслуговують на увагу алгоритми ущільнення, які формують масиви символів перед виконанням ущільнення, що може бути використано при реалізації алгоритму шифрування. Іншими важливими критеріями є адаптивність алгоритму ущільнення, коефіцієнт ущільнення, простота технічної реалізації. Характеристики основних методів ущільнення за даними критеріями наведені в табл. 1.

Таблиця 1 – Характеристики методів ущільнення

Метод ущільнення	Коефіцієнт ущільнення	Обчислювальні затрати	Адаптивний	Додаткові обчислювальні затрати для шифрування
Словниковий	Близький до оптимального для великих масивів	Середні	Так	Так
Хаффмана	Оптимальний	Середні	Ні	Так
MTF	Близький до оптимального	Середні	Так	Ні
Імовірнісний	Близький до оптимального	Малі	Так	Ні
Арифметичний	Найбільший	Великі	Так	Так

Як видно з таблиці серед розглянутих алгоритмів ущільнення найбільші переваги, з точки зору застосування їх до шифрування даних, мають два алгоритми:

- ущільнення методом MTF (Move To Front);
- ймовірнісний метод ущільнення.

Ці алгоритми передбачають формування таблиці символів перед виконанням ущільнення даних, яка може бути сформована за ключем шифру з використанням, наприклад, генератора псевдовипадкових чисел. До того ж ці алгоритми є адаптивними, тобто не вимагають передачі додаткової інформації, яка могла бути використана зломисниками для злому шифру, а також характеризуються простою технічною реалізацією.

Наприклад, для одночасного ущільнення з використанням MTF-кодування і шифрування методом багатоалфавітної підстановки може використовуватись така схема:

1. З використанням генератора псевдовипадкових чисел генерується алфавіт повідомлення. Оскільки символи в комп'ютерних системах подані восьмибітовими комбінаціями, то генератор повинен забезпечувати довжину не менше чим 256, а породжувальне число генератора можна вводити як ключ шифру.

2. Виконується ущільнення методом MTF з використанням згенерованого алфавіту.

Список літератури:

1. Майданюк В. П. Кодування та захист інформації. - Вінниця: ВНТУ, 2009. - 164 с.
2. Майданюк В. П. Ущільнення даних як метод криптографічного захисту / Методи та засоби кодування, захисту й ущільнення інформації. Тези доповідей Третьої Міжнародної науковопрактичної конференції. м. Вінниця, 20-22 квітня 2011 року. – Вінниця: ВНТУ, 2011. – С. 98-99.

РОЛЬ РЕАЛЬНОГО ДИПЛОМНОГО ПРОЕКТУВАННЯ У ПІДГОТОВЦІ ФАХІВЦІВ З АВТОМАТИЗАЦІЇ

**Максименко А.О., Лящев Ю.Ю., студенти 4 курсу,
Керівник Зігунов О.М., к.т.н.
Сумський коледж харчової промисловості НУХТ**

З переходом до третього тисячоліття науково-технічний прогрес заграє новими барвами. Нові технології з'являються не щорічно, а щоденно, а в купі з ринковою економікою підприємства різко почали потребувати висококваліфікованих працівників.

**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.