МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ITSec-2023

Безпека інформаційних технологій

МАТЕРІАЛИ

XII Міжнародної науково-технічної конференції

2-4 травня 2023
м. Ужгород (Україна)

УДК [003.26+004+519.816]:004.056:65(063)

ITSec: Безпека інформаційних технологій: матеріали XII Міжнар. наук.-техн. конф., м. Ужгород, 2-4 жовт. 2023 р. К.: НАУ, 2023. 140 с.

Збірник містить тексти наукових матеріалів доповідей та тез учасників XII міжнародної науково-технічної конференції «ITSec: Безпека інформаційних технологій». Основною метою конференції є ознайомлення з сучасними досягненнями та висвітлення результатів наукових досліджень з усіх аспектів кібербезпеки та захисту інформації.

Призначено вченим, інженерам, аспірантам наукових спеціальностей 05.13.21 – Системи захисту інформації, 21.05.01 – Інформаційна безпека держави, здобувачам вищої освіти за спеціальностями: 125 – Кібербезпека, а також всім зацікавленим.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

- Національний авіаційний університет
- ДВНЗ «Ужгородський національний університет»
- Казахський національний педагогічний університет ім. Абая
- Кафедра безпеки інформаційних технологій НАУ
- Кафедра твердотільної електроніки та інформаційної безпеки УжНУ
- Наукова школа “Кібербезпека” НАУ
- ГО “Асоціація спеціалістів кібербезпеки”
- ТОВ «Безпека інформаційних систем «Дельта»
- Редакція наукового журналу «Безпека інформації»
- Редакція наукового журналу «Захист інформації»

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

Співголови	**Максим ЛУЦЬКИЙ**, д.т.н., проф., ректор Національного авіаційного університету
	Володимир СМОЛАНКА, д.м.н., проф., ректор ДВНЗ «Ужгородський національний університет»
Заступники співголов	**Олександр Корченко,** д.т.н., проф., зав. каф. БІТ НАУ
	Василь РІЗАК, д.ф.-м.н., проф., зав. каф. ТЕІБ УжНУ
Відповідальні секретарі	**Юлія ХОХЛАЧОВА**, к.т.н., доц., доц. каф. БІТ НАУ
	Михайло ПРИГАРА, к.т.н., доц. каф. ТЕІБ УжНУ
	Марина ПОГОРЕЛОВА, асистент каф. БІТ НАУ

Члени програмного комітету

Микола КАРПІНСЬКИЙ, д.т.н., проф.,
Університет у Бєльсько-Бялій (м. Бєльсько-Бяла, ПОЛЬЩА)
Станіслав РАЙБА, д.т.н., проф.,
Університет у Бєльсько-Бялій (м. Бєльсько-Бяла, ПОЛЬЩА)
Бахитжан АХМЄТОВ, д.т.н., проф.,
Казахський національний педагогічний університет ім. Абая (м. Алмати, КАЗАХСТАН)
Геворг МАРҐАРОВ, к.т.н., доц.,
Державний інженерний університет Вірменії (м. Єреван, ВІРМЕНІЯ)
Володимир МОХОР, д.т.н., проф. чл.-кор. НАН України,
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова, НАН України (м. Київ, УКРАЇНА)
Олена ТИМОШЕНКО, д.ф.н. проф.,
Європейський Університет (м. Київ, УКРАЇНА)
Євген ВАСІЛІУ, д.т.н., проф.,
Державний університет інтелектуальних технологій і зв'язку (м. Одеса, УКРАЇНА)
Василь ЦУРКАН, ктн. доц.,
Національний технічний університет України "Київський політехнічний інститут ім. Ігоря Сікорського" (м. Київ, УКРАЇНА)

РФС спектри наношару тиміну на модельних поверхнях окису титану показали, що пік основного рівня нітрогену N 1s зміщується в бік нижчих енергій на $\Delta E_{зв}$=-(0.3+ +0.7) еВ відповідно після відпалу при T>100˚C . Такі енергетичні зсуви в органічних багатошарових покриттях пояснюються утворенням хімічних зв'язків між молекулами та підкладкою (хемосорбцією). Пік основного рівня C 1s плівки тиміну містить чотири компоненти, які відповідають карбону з вуглеводними зав'язками C-C, C-H; карбону, зв'язаному з азотом C-N, N-C-N; амідному карбону N-C=O; уреа карбону N-C{=O}-N з енергіями зв'язку 285, 285,7; 286,5 та 289,2 еВ відповідно. Для плівки тиміну пік основного рівня C 1s поступово зміщується в бік нижчих значень енергії зв'язку на 0.7-0.4 еВ після відпалу при T>100-120˚C. При цьому товщина шару тиміну в результаті відпалу при температурах до 200˚C не змінювалася.

Наношар гуаніну на поверхні монокристалічного (110) TiO_2 виявився стійким до відпалу при температурах до 450˚C.

Висновок: результати дослідження фотоелектронних спектрів наношарів азотистих основ ДНК на модельних поверхнях показали широкий спектр особливостей геометричної та електронної структури досліджуваних матеріалів, які можуть бути використані при розробці методів ДНК-криптографії та визначати галузі їх використання. Для розробки теоретичних основ застосування ДНК та її основ у молекулярній криптографії, а також чіткого механізму взаємодій та перетворень, які цих об'єктів під впливом сторонніх факторів предметом наших подальших досліджень є характеристики цитозину на модельних поверхнях, а також поведінка шарів окремих нуклеотидів при тиску повітря, близькому до атмосферного, тобто в умовах, максимально наближених до умов функціонування майбутніх пристроїв на основі ДНК.

УДК 004.421.5.052

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ WEB-РЕСУРСІВ СТІЙКИМИ КРИПТОАЛГОРИТМАМИ НА ОСНОВІ ГЕНЕРАТОРІВ ВИПАДКОВИХ ЧИСЕЛ

Ольга Салієва[1], Василь Карпінець[1], Ірина Бондаренко[1]
[1]Вінницький національний технічний університет
salieva8257@gmail.com, karpinets@gmail.com,
fm.ub15b.bondarenko@gmail.com

Широке впровадження Web-технологій в усі сфери людської діяльності обумовлює вагомість вирішення питань щодо їхньої безпеки. Адже на сьогодні безліч Web-застосунків мають загальновідомі вразливості, за допомогою яких можна успішно проводити атаки на Web-ресурси.

З метою підвищення захищеності Web-інфраструктури використовують різні методи і засоби, зокрема стійкі криптографічні алгоритми на основі генераторів випадкових чисел (ГВЧ), які поділяються на: апаратні, програмні та табличні. Останні мають багато переваг, зокрема видають істино випадкову послідовність, не потребуючи фізичної наявності модуля генерації у системі. Проте для зберігання таблиць потрібний великий обсяг пам'яті ЕОМ. Для вирішення даної проблеми у роботі пропонується використати ентропію поведінки користувача в якості Seed даних табличного ГВЧ, оскільки таке джерело ентропії є швидкодіючим та фактично нескінченим.

Метою даної роботи є підвищення захищеності Web-ресурсів за рахунок стійких криптографічних алгоритмів на основі ГВЧ, що враховують ентропію поведінки користувача у багатокористувацькому середовищі.

Для досягнення мети досліджено алгоритм надійного джерела ентропії на основі поведінки користувача Web-ресурсу та об'єднано окремі модулі ГВЧ, а саме алгоритм заповнення буфера табличного ГВЧ та алгоритм вибору з нього випадкового числа.

Розроблений алгоритм умовно розподілено на два етапи.

Етап 1. Заповнення буферу табличного ГВЧ.

Крок 1. В якості показників ентропії обираються координати курсора користувача X та Y.

Крок 2. Обчислюється $Z_n = X_n \oplus Y_n$, яке є результатом ентропії поведінки користувача.

Крок 3. Перевіряється рівність Z_n та Z_{n-1}.

Крок 4. Надсилається Z_n з клієнтської частина на сервер.

Крок 5. На стороні сервера розраховується $Q = Z_{An} \oplus Z_{Bn}$, де Z_{An} – значення ентропії користувача A, а Z_{Bn} – значення ентропії користувача B.

Крок 6. У комірку таблиці з індексом i записується Q.

Крок 7. Інкрементується та записується i.

Крок 8. Здійснюється перевірка: якщо i більше розміру таблиці, то йому присвоюється значення 0.

Етап 2. Вибір випадкового числа.

Крок 1. У модуль передається бажана довжина послідовності n.

Крок 2. З комірки таблиці з індексом i вибирається число X_i.

Крок 3. Інкрементується та записується i.

Крок 4. Перевіряється чи довжина числа X_i задовольняє бажаному n.

Крок 5. Якщо довжина X_i менша n, то вибирається наступне число X_{i+1} (повторюються кроки 2, 3) та конкатинується до X_i.

Числа вибираються та конкатинуються до тих пір, доки довжина числа X_i не задовольняє бажаному n n.

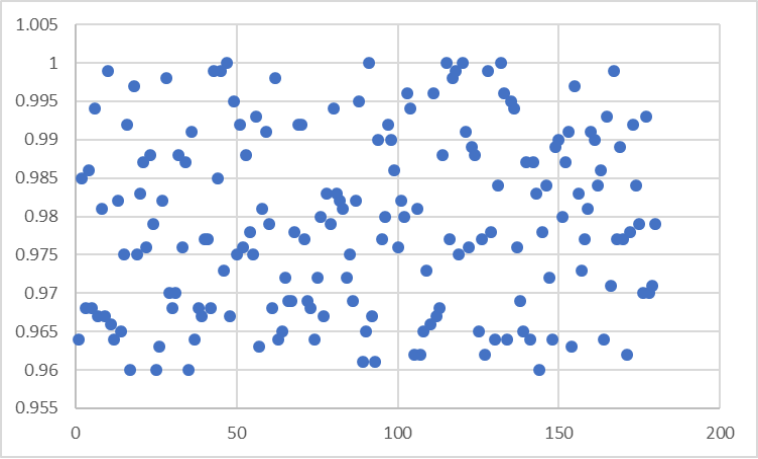

Рис. 1. Результати тестування послідовності згенерованої розробленим ГВЧ

На основі запропонованого алгоритму роботи ГВЧ було розроблено пакет програм криптографічної підсистеми захисту інформації, зокрема, здійснено програмну реалізацію серверної частини алгоритму табличного ГВЧ для платформи ASP.NET Core та клієнтської для Angular2.

Крім того, було здійснено статистичне тестування згенерованої послідовності за допомогою пакету NIST.

На рис. 1 представлена діаграма, що характеризує попадання частки послідовностей, що пройшли кожен тест у довірчий інтервал [0,96; 1].

Отриманий результат підтвердив, що дана послідовність задовольняє відповідним критеріям випадковості.

Таким чином, за рахунок використання розробленого табличного ГВЧ, який враховує ентропію поведінки користувача, можна підвищити стійкість криптографічних алгоритмів, що, у свою чергу, сприятиме підвищенню захищеності Web-ресурсів.

УДК 004.056.52

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ МЕТОДІВ РОЗМЕЖУВАННЯ ДОСТУПУ В ІНФОРМАЦІЙНОМУ ПРОТИБОРСТВІ

Анатолій Шиян[1], Михайло Тюльпін[1], Яна Яремчук[1]
[1]Вінницький національний технічний університет,
[1]anatoliy.a.shiyan@gmail.com, mtyulpin@gmail.com, yanunova@hotmail.com