

The 12th International Scientific Conference «ITSec» May, 2-4 2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ
УНІВЕРСИТЕТ

ITSec-2023

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»

~ 3 ~

The 12th International Scientific Conference «ITSec» May, 2-4 2023

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 співголови 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 Бельсько-Бялій (м. Бельсько-Бяла, ПОЛЬЩА)

Станіслав РАЙБА, д.т.н., проф.,

Університет у Бельсько-Бялій (м. Бельсько-Бяла, ПОЛЬЩА)

Бахитжан АХМЕТОВ, д.т.н., проф.,

Казахський національний педагогічний університет ім. Абая (м. Алмати, КАЗАХСТАН)

Геворг МАРГАРОВ, 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 ВАСІЛУ, 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)

~ 4 ~

The 12th International Scientific Conference «ITSec» May, 2-4 2023 **ЗМІСТ**

Аkhmetov Bakhytzhан, Lakhno Valeriy, Adilzhanova Saltanat
Dynamic management of cybersecurity resources based on genetic algorithms.....9
Віталій Біланич, Олег Шиленко, Василь Біланич, Alexander Feher, Vladimir Komanicky, Василь Різак
Виготовлення захисних елементів на халькогенідних плівках методом електронної літографії.....15
Володимир Богом'я, Юлія Літвінова, Максим Залевський Деякі особливості машинного навчання, як технології бізнес-аналітики.....17
Анатолій Давиденко, Олена Висоцька

Фіксація деструктивної дезінформації в кіберпросторі за участі студентів спеціальності «Кібербезпека».....19
Сергій Гільгурт
Використання ПЛІС для захисту кіберфізичних систем енергетики.....22
Володимир Хорошко, Юлія Хохлачова, Наталія Вишневська
Алгоритм структурної ідентифікації прогнозуючих моделей.....23
Богдан Маліцький, Олександр Черепов, Василь Буковецький, Василь Різак
Полігон для проведення комплексних навчань з багаторівневого захисту від кібератак.....27
Олег Карабан
Дослідження та порівняння систем моніторингу комп'ютерних систем і мереж.....28
Аль-Амморі Алі, Сергій Заворотний
Оцінка ефективності захисту інформації в транспортній галузі.....30
Микола Карпінський, Олександр Корченко, Юрій Дрейс
Побудова моделі первинних параметрів оцінки стану охорони державної таємниці.....32
Віта Каштан
Алгоритм шифрування зображень дистанційного зондування Землі з використанням двоканальної передачі ключів.....34
Юлія Мисло, Михайло Пагіря
Криптоаналіз асиметричних ключів алгоритмами ланцюгових дробів36
Богдан Савенко, Антоніна Каштальян, Наталія Петляк
Розподілені системи виявлення worm-вірусів.....37

Роман Ситник, Вікторія Гнатушенко
Забезпечення безпеки доступу до хмарних обчислень за допомогою блокчейн технологій.....39
Роман Штонда, Юлія Черниш, Ірина Мальцева
Захист інформації та кібербезпека в радіорелейних лініях зв'язку41
Ірина Удовик, Володимир Гнатушенко

~ 5 ~

The 12th International Scientific Conference «ITSec» May, 2-4 2023

Використання квантового машинного навчання при обробці багатоканальних аерокосмічних зображень.....42
Дмитро Євграфов, Юрій Яремчук
Енергоощадне придушення каналів витоку інформації з екранів моніторів на рідинно-кристалічних структурах.....44
Сергій Зибін
Ризики в апаратному забезпеченні.....46
Ольга Васильєва
Імітаційні моделі при моделюванні інформаційних операцій у соціальних мережах.....48
Віта Каштан, Денис Іванов, Ольга Коробко
Кібербезпека віртуальних грошей в епоху цифрової економіки.....50
Олександр Кручинін, Володимир Святошенко, Дмитро Тимофєєв
Особливості автоматизованих систем управління дорожнім рухом як об'єктів кіберзахисту.....52
Володимир Святошенко, Олександр Кручинін, Дмитро Тимофєєв

Порівняльний аналіз відкритих платформ з кібербезпеки.....	54
Дмитро Тимофєєв, Олександр Кручінін, Володимир Святошенко	
Реалізація архітектури нульової довіри в процесі впровадження системи управління інформаційною безпекою закладів вищої освіти України.....	56
Іван Трикур, Михайло Січка , Олександр Чобаль, Галина Різак, Василь Різак	
Багатофункціональні оптичні елементи на основі бактеріородопсину у системах контролю доступу та інформаційної безпеки.....	58
Роман Гамрецький, Костянтин Зандер	
Аналіз метрик кібербезпеки для оцінювання якості програмного забезпечення в інформаційно комунікаційних системах.....	60
Roman Karpiuk, Petro Venherskyi	
Using machine learning (ml) to detect threat anomalies for reducing false-positives on the daily cybersecurity operation centre routine.....	62
Valerii Kozlovskiy, Svitlana Nimych, Oleksii Komar	
Use of inhomogeneous lines as a filtering element for design of SHF devices.....	64
Михайло Кишак	
Проект пристрою активного захисту мовної інформації на базі генератора шуму.....	66
Kateryna Nesterenko, Oleksii Nimych, Vladyslav Dudnyk	
Determination of a four-pole transmission line matrix based on a nonuniform.....	67
Євгенія Іванченко, Ігор Іванченко, Ірина Лозова, Євгеній Педченко, Марі Петровська	
Архітектура хмарного рішення для централізованого збору та обробки інцидентів інформаційної	

безпеки..... 69
Пішковцій Марія-Ольга, Різак Василь
Молекулярна криптографія в кібербезпеці73
Сергій Базарний
Удосконалення методики оцінювання ефективності психологічного впливу в інформаційній операції..... ...76
Любомир Боценюк, Юрій Матьовка Віддалений контроль і захист персонального комп'ютера від несанкціонованого доступу на основі телеграм бота..... 78
Валерій Ворожко
Безпечкові ризики під час транспортування носіїв тасмної інформації гужовим транспортом..... 80
Максим Делембовський
OSINT – елемент розвідки в умовах кібервійни..... 82
Іванов Денис
Метод двійного хещування SHA з додатковим перебором..... 84
Павло Ігнатоля, Ярослав Сивохоп, Василь Різак
Класифікація та аналіз загроз в інтелектуальних транспортних системах..... 86
Каблучко Дмитро
Захист критичної інформаційної інфраструктури та банків..... 88
Володимир Лужецький

Псевдонедетермінований підхід до побудови шифрів.....90
В.О. Крайнов
Мережево-центрична парадигма інформаційної безпеки в автоматизованих інформаційних системах управління військового призначення.....92
Володимир Шиповський
Порівняльний аналіз логічних моделей оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури.....95
Наталія Петляк, Юлія Хохлачова, Юрій Кльоц
Підхід до аналізу вихідного графіку.....97
Єгор Шарай, Георгій Чупрін
Приватність та інформаційна безпека у соціальних медіа.....99
Михайло Пригара, Іван Опірський, Михайло Різак
Оцінка виявлених ризиків інформаційної безпеки в освіті в умовах надзвичайних ситуацій.....105
Віталій Тупкало, Сергій Черепков
Сигнатурний метод контролю ходу програм цифрових автоматів.....109

~ 7 ~

The 12th International Scientific Conference «ITSec» May, 2-4 2023

Анатолій Грицак, Ігор Абрамчук, В. Саврацький
Підвищення захищеності Web ресурсу від атак типу Cross-Site Scripting.....111
Богдан Карачун
Управління інцидентами інформаційної безпеки за допомогою SIEM.....113

Павло Павловський, Дмитро Присяжний, Віталій Гудзь	
Виявлення радіозакладних пристроїв за рахунок поєднання методів локалізації за рівнем поля та акустичного зв'язування.....	115
Наталія Попович, Наталія Цуд, Катеріна Велтруска, Владімір Матолін, Василь Різак	
Виготовлення та властивості наношарів азотистих основ нуклеїнових кислот для молекулярної криптографії.....	.117
Ольга Саліса, Василь Карпінєць, Ірина Бондаренко	
Підвищення захищеності Web-ресурсів стійкими криптоалгоритмами на основі генераторів випадкових чисел.....	119
Анатолій Шиян, Михайло Тюльпін, Яна Яремчук	
Перспективи використання методів розмежування доступу в інформаційному протиборстві.....	
121	
Василь Буковецький, Юрій Тягур, Тетяна Матювка	
Інструменти для зневадження клієнт-серверних застосунків.....	123
Марина Сасенко	
Виникнення загроз у кіберпросторі як результат технологічного розвитку суспільства.....	
124	
Lakhno V., Malyukov V., Akhmetov B., Alimseitova Zh., Ogan A.	
Strategy of countering phishing attacks on the cryptocurrency exchange as part of the endless antagonistic game scheme.....	127
Юлія Хохлачова, Алла Гаврилова	
Проблеми безпеки інформації в сучасних інформаційно-комунікаційних системах та мережах.....	
128	
Людмила Ковальчук, Роман Олійников, Юрій Беспалов, Ганна Неласа	
Розвиток криптографічних протоколів анонімної маршрутизації в Інтернет.....	
130	

Dora Sabov, Pavlo Mulesa, Marianna Sharkadi
The State of Cyber Security of Ukraine During a Full-Scale Intrusion.....132
Віталій Носов, Василь Лучик, Тетяна Колісник, Сергій Калякін, Віталій Світличний
Оцінка реалізації розподіленого криптоаналізу в умовах обмежених ресурсів.....134
Євгенія Галич , Владислав Павленко
Штучний інтелект Chat GPT: можливості та загрози технологічної новинки.....139

~ 8 ~

The 12th International Scientific Conference «ITSec» May, 2-4 2023

UDC 32.973.202 (004.8)

**DYNAMIC MANAGEMENT OF CYBERSECURITY RESOURCES
BASED ON GENETIC ALGORITHMS**

Akhmetov Bakhytzhn, Lakhno Valeriy, Adilzhanova Saltanat

Kazakh National Pedagogical University named after Abai¹, National
University of Bioresources and Occupational Sciences of Ukraine²,
Al-Farabi Kazakh National University³

¹b.akhmetov@abaiuniversity.edu.kz, ²lva964@nubip.edu.ua,
³asaltanat81@gmail.com

The report examines methods, models and information technologies for the dynamic management of cybersecurity resources. The relevance of the study is determined by the need to optimize the indicators of information security tools of the object of informatization (OBI) in the conditions of dynamic confrontation with the attacking party. The solution to the problem is seen in the optimal distribution of limited financial resources of the OBI management between the objects of protection, taking into account the actions of the attacker.

The problem of dynamic resource management of the OBI protection side is not only a purely technical task, which is solved by increasing the number of protection components in the cybersecurity circuits (KB) of the OBI. But it's also a management challenge. Moreover, the second component of the tasks is associated with such a concept as information security management (IS) and KB, the main task of which is to optimize not only technical, but also economic indicators of the effectiveness of the functioning of information security tools (SIR) for OBI [1].

The criterion of optimality can be one (or several) indicators of information

УДК 539.23, 538.958, 004.056.53

БАГАТОФУНКЦІОНАЛЬНІ ОПТИЧНІ ЕЛЕМЕНТИ НА ОСНОВІ БАКТЕРІОРОДОПСИНУ У СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

**Іван Трикур¹, Михайло Січка², Олександр Чобаль³,
Галина Різак⁴, Василь Різак⁵**

ДВНЗ «Ужгородський національний університет»

¹ivan.trikur@uzhnu.edu.ua, ²mykhaylo.sichka@uzhnu.edu.ua,

³oleksandr.chobal@uzhnu.edu.ua, ⁴galyna.rizak@uzhnu.edu.ua,

⁵vrizak@uzhnu.edu.ua

Актуальність проблематики вдосконалення систем інформаційної безпеки важко переоцінити. Одним з невід'ємних елементів розвитку таких систем є розробка та створення їх матеріальної бази. Бактеріородопсин (БР), який володіє рядом цікавих властивостей, є одним з біологічних матеріалів, що можуть бути ефективно використані у даному напрямку. Від більшості білків він відрізняється структурною організацією молекул у вигляді двомірних кристалів, завдяки чому, демонструє набагато більшу, порівняно з іншими білками, фізичну та хімічну стабільність. Завдяки цьому для БР можливі способи практичного використання, які не можуть бути використані для інших білків. Комбінація оптичних властивостей БР з іншими матеріалами дозволяє отримати функціональні елементи, які можуть бути використані у системах інформаційної безпеки.

Метою даної роботи є систематизація, аналіз та узагальнення даних про можливості використання матеріалів на основі БР у багатофункціональних оптичних елементах систем контролю доступу та інформаційної безпеки.

Поглинання одного кванту світла приводить до збудження молекули БР, після чого, через ряд проміжних станів - інтермедіатів, вона повертається у вихідний стан. Інтермедіати відрізняються спектрально і часами життя. Одним з таких проміжних станів є інтермедіат K_{610} , який стабільний при температурах нижче 150 К. Переходи між BP_{570} і K_{610} можуть ініціюватися при опроміненні

молекули світлом відповідної довжини, що дозволяє створити бінарну фотохімічну систему на основі даних двох станів. Висока квантова ефективність ($BP \rightarrow K=65\%$, $K \rightarrow BP=80\%$) фотопереходів відкриває можливість створення криогенних запам'ятовуючих пристроїв, які володіють високою швидкодією та ефективністю. Аналогічну систему можна реалізувати на основі переходу $BP_{570} \leftrightarrow M_{412}$. Для даної фотореакції характерний більший спектральний зсув між станами та високі квантові ефективності ($BP \rightarrow M=65\%$, $M \rightarrow BP=65\%$). При температурах вище 240 K інтермедіат M_{412} термічно нестабільний і молекула переходить в основний стан протягом кількох мілісекунд. Високі перерізи двофотонного поглинання роблять можливим 3-D запис інформації, що суттєво збільшує ємність носіїв. Висока роздільна здатність дозволяє реалізовувати голографічний посторінковий запис інформації з адресацією за змістом, який не може бути реалізований за допомогою звичайної електроніки. Носії на інтермедіатах K_{610} та M_{412} можуть знайти застосування коли зберігання секретних даних вимагає їх лабільності для

~ 58 ~

The 12th International Scientific Conference «ITSec» May, 2-4 2023

запобігання несанкціонованому доступу. Остання можливість пов'язана з тим фактом, що всі дані, які зберігаються в інтермедіатах K або M , будуть безповоротно втрачені при нагріванні носія вище ніж 150 та 240 K відповідно.

При лазерному опроміненні молекула BP може поглинути два фотони, що призводить до утворення фотопродукту F_{620} , який не повертається у вихідний стан. Поляризований лазерний імпульс при взаємодії з іммобілізованим BP індукуює постійну фотоіндуковану анізотропію, що може бути використано для поляризаційного запису. Точки даних можуть записуватися різною поляризацією, наприклад 0° – "1", 90° – "0". Інформацію, записану у вигляді зміни поляризаційних властивостей середовища, важко скопіювати. Роздільна здатність середовища в поєднанні з наведеним способом запису дозволяє здійснювати кутове мультиплексування, що може суттєво збільшувати густину запису та ускладнювати її копіювання. Крім прямого оптичного запису даних BP дає можливість оптичного шифрування даних. При записі обох видів поляризації в одному місці матеріал втрачає анізотропію. Поляризація в таких точках не може бути зчитана, що, у свою чергу, не дає можливості інтерпретувати її як «0» або «1». Це означає, що набір двійкових даних, який має бути зашифрований, перезаписується другим набором даних, який служить «ключем» для шифрування. У всіх бітах, де дані та ключ співпадають, накладена точка даних не змінюється. Але в позиціях де значення бітів даних і ключа не співпадають – анізотропія стирається. Інформація може бути відновлена тільки якщо відомий ключ.

Реверсивний фотохромний зсув поглинання у видимій області при переході $BP_{570} \leftrightarrow M_{412}$ під дією освітлення, дозволяє отримувати фотохромні чорнила для захисного маркування та виготовлення фотохромних областей на картах доступу чи перепустках. Реологічні характеристики таких чорнил подібні до комерційних. Реверсивна зміна кольору дозволить унеможливити несанкціоноване копіювання документів або/та верифікувати відповідне маркування продукції. Використання барвників в стехіометричному співвідношенні з молекулами BP дозволяє отримати повний спектр кольорових відтінків при збереженні фотохромності матеріалу.

Наявність всього спектру чорнил полегшить інтеграцію елементів захисту в будь який документ.

Зміну кольору чи наявність поляризаційно записаної інформації можна помітити неозброєним оком. Однак матеріали на основі БР дозволяють створити захисні елементи, які можна проаналізувати лише в лабораторних умовах. Зокрема можна реалізувати можливість відстеження партій товару виготовленого чи маркованого з використанням БР. Для цього нефункціональні частини амінокислотного ланцюга можна модифікувати, наприклад, заміною певних амінокислотних залишків. Така модифікація виявляється лише мас спектроскопічними методами та дозволяє надійно ідентифікувати походження матеріалу.

Всі перераховані можливості можуть бути реалізовані в багатофункціональних (як видимих так і не видимих) елементах захисту на одній ID-карті. Перераховані вище факти свідчать, що фотохромні матеріали на основі БР можуть ефективно використовуватися у сфері інформаційної безпеки та контролю доступу.

~ 59 ~

The 12th International Scientific Conference «ITSec» May, 2-4 2023