

Державна служба України з надзвичайних ситуацій
Національний університет цивільного захисту України

З В Д А П О Б І Г Т И Р Я Т У В А Т И О П О М О Г Т И

Матеріали міжнародної науково-практичної
конференції молодих учених
«Проблеми та перспективи
забезпечення цивільного захисту»



ХАРКІВ 2024

**ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ**

МАТЕРІАЛИ

**міжнародної науково-практичної конференції
молодих учених**

**«Проблеми та перспективи
забезпечення цивільного захисту»**

Харків – 2024

УДК 614.8

Проблеми та перспективи забезпечення цивільного захисту: матеріали міжнародної науково-практичної конференції молодих учених. Харків: НУЦЗУ, 2024. 558 с. Українською та англійською.

Включено матеріали, які доповідались на міжнародній науково-практичній конференції молодих учених на базі Національного університету цивільного захисту України.

Розглядаються аспекти вдосконалення цивільного захисту держави.

Матеріали розраховані на інженерно-технічних працівників Державної служби України з надзвичайних ситуацій, науково-педагогічний склад, ад'юнктів, слухачів, студентів та курсантів закладів вищої освіти України та інших країн світу.

СКЛАД ОРГКОМІТЕТУ КОНФЕРЕНЦІЇ

Голова:

ГВОЗДЬ

Віктор

т.в.о. ректора Національного університету цивільного захисту України, кандидат технічних наук, професор, Заслужений працівник цивільного захисту України

Заступник голови:

АНДРОНОВ

Володимир

проректор з наукової роботи Національного університету цивільного захисту України, доктор технічних наук, професор, Заслужений діяч науки і техніки України

Члени оргкомітету:

DIMITAR

Georgiev

Head of Scientific Research Center for Disaster Risk Reduction University of National and World Economy, Doctor of Science, Professor (Republic of Bulgaria)

САЄНКО

Сергій

начальник відділу газостатичних та плазмових технологій Національного наукового центру «Харківський фізико-технічний інститут», доктор технічних наук, старший науковий співробітник

KRONIN

Maykl

Professor of the Department of Social Work at Monmouth University, International Instructor of Psychological Assistance in Emergency Situations of the American Red Cross (USA)

МАНДИЧ

Олександра

голова ради молодих вчених при харківській обласній державній адміністрації, доктор економічних наук, професор

SILOVS

Marek

Deputy Head of the College of Fire Safety and Civil Protection of Latvia (Republic of Latvia)

ДАДАШОВ

Ільгар

Академія МНС Азербайджанської Республіки, доктор технічних наук, доцент (Азербайджанська Республіка)

TIKHONENKOV

Igor

Department of Chemistry, Ben Gurion University of the Negev, Be'er Sheva, PhD (Israel)

ПОРІВНЯННЯ ШВИДКОДІЇ НМАС АЛГОРИТМІВ

Малярова Д.М., ХНУРЕ
НК – Малярів М.В., к.т.н., доцент, НУЦЗУ

На сьогоднішній день інформаційні технології стали невід'ємною частиною суспільства, забезпечуючи збір, зберігання та обмін даними. Розвиток криптографії та програмного захисту інформації набуває все більшого значення, але викликом залишається постійне покращення їхньої надійності.

Автентифікація (англ. authentication) – процедура перевірки відповідності пред'явленого ідентифікатора об'єкта комп'ютерної системи на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності [1].

Коди автентифікації, або MAC-коди (англ. message authentication code) – криптографічні геш-функції, для обчислення яких необхідно знати секретний ключ, використання якого дозволяє гарантує неможливість підміни захищених об'єктів. MAC-коди дуже корисні для перевірки автентичності без порушення безпеки [2].

НМАС (ISO/IEC 9797-1) – MAC-код на основі геш-функції, що має таку перевагу, що дозволяє повторне використання існуючих реалізацій геш-функції. MAC-коди на основі геш-функції та секретного ключа найбільш загальні методи, оскільки вони звичайно швидше, ніж коди на основі блокового шифру [3].

При реалізації НМАС можуть використовуватися різні функції гешування, такі як Whirlpool, MD4, MD5, RIPEMD, SHA-0, SHA-1, SHA-2 (SHA-256, SHA-384, SHA-512), Tiger та інші. Швидкість обчислень визначається кількістю циклів процесора, затрачуваних на один байт оброблюваного повідомлення [3]:

- Алгоритм НМАС-Whirlpool, НМАС-SHA-512 мають найбільшу довжину коду та довжину ключа. А найбільшу довжину ключа, але найкоротшу довжину коду мають алгоритми НМАС-MD4 та НМАС-MD5.

- Найшвидшим алгоритмом на усіх типах процесора (Pentium2, PIII/Linux, Pentium4, Xeon, AMD) є НМАС-MD4, а другим за швидкістю є НМАС-MD5. Найповільнішими є алгоритми НМАС-SHA-384 і НМАС-SHA-512.

Довжина коду та довжина ключа можуть змінюватися залежно від алгоритму гешування та типу процесора. Загалом, алгоритми з більшою довжиною коду більш безпечні, але вимагають більше обчислювальних ресурсів.

Таким чином, автентифікація, шифрування даних та використання кодів автентифікації (MAC-кодів) забезпечують безпеку під час обробки та передачі даних, дозволяючи перевіряти автентичність та запобігати підробкам. Алгоритми НМАС, базовані на різних функціях гешування, є ефективними та універсальними методами для створення кодів автентифікації, дозволяючи забезпечити безпеку інформації у сучасних інформаційних системах.

ЛІТЕРАТУРА

1. Захарченко М. В. Асиметричні методи шифрування в телекомунікаціях: навч. посіб. М. В. Захарченко, О. В. Онацький, Л. Г. Йона, Т. М. Шинкарчук. Одеса: ОНАЗ ім. О. С. Попова, 2011. 184 с.
2. Шнаер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. Б. Шнаер. 2-е изд. М.: ТРИУМФ, 2001. 308 с.
3. Євсєєв С. П. Гешування даних в інформаційних системах: монографія. С. П. Євсєєв, О. Ю. Йохов, О. Г. Король. Х.: Вид. ХНЕУ, 2013. 312 с.

<i>Малярова Д.М., ХНУРЕ</i> Порівняння швидкодії НМАС алгоритмів.....	256
<i>Метьюлкін О.О., НУЦЗУ</i> Доцільність комп'ютеризації окремих аспектів методології відкритого коду гуманітарного розмінування.....	257
<i>Підкопай О.Ю., НУЦЗУ</i> Залежність динамічних параметрів сповіщувача від параметрів чутливого елемента.....	258
<i>Пісарев В.О., Устїнов В.В., НУЦЗУ</i> Аналіз стану та тенденції удосконалення пожежної автоматики України.....	259
<i>Пономарьов К.А., НУЦЗУ</i> Формалізація обмежень при формуванні шлейфів пожежної сигналізації.....	260
<i>Радул А.Ю., НУЦЗУ</i> Перспективи використання систем пожежогасіння тонкорозпиленою водою для захисту висотних будівель.....	261
<i>Семків В.О., НУЦЗУ</i> Основні вимоги до пожежно-рятувального автомобіля.....	262
<i>Скрипник А.В., НУЦЗУ</i> Метод отримання рівняння динаміки теплового пожежного сповіщувача.....	263
<i>Степанчук С.О., НУЦЗУ</i> Визначення задач, вирішення яких потребує розробка оперативної-технічної методики гуманітарного розмінування в радіаційно-забрудненій місцевості.....	264
<i>Федоренко Є.Р., Шинкаренко А.С., НУЦЗУ</i> Застосування карт кохонена в завданні розізнавання джерел заморювання.....	266
<i>Філіпенко Є.О., НУЦЗУ</i> Аналіз стану та напрямів удосконалення методів випробувань установок пожежогасіння.....	267
<i>Чеголя А.В., НУЦЗУ</i> Щодо оповіщення населення в умовах воєнного стану.....	268
<i>Шахов С.М., НУЦЗУ</i> Дослідження зниження густини кисню на шляхах евакуації у PYROSIM.....	269
<i>Шинкаренко А.С., Федоренко Є.Р., НУЦЗУ</i> Базові доктрини спецтехнологій утворення корпоративних сховищ даних.....	270
<i>Berezan M., NUCDU</i> Social networks.....	271
<i>Bondarenko A., NUCDU</i> The problem of preventing emergency situations related to the release of pollutants into the environment.....	272
<i>Chyzhyk M., NUCDU</i> Determination of the amount of oil residues in vertical steel reservoirs.....	273
<i>Korchagin P., NUCDU</i> Overview of the problems of the system of training specialists in the operation of emergency and rescue equipment during wartime.....	274
<i>Myroshnychenko A., NUCDU</i> Problems of warning of emergency situations and fire in tunnels.....	275
<i>Shcherbak O., NUCDU</i> Problems of detecting central signs of an emergency due to fire at critical infrastructure facilities.....	276
<i>Vovchuk T., NUCDU</i> Problems of information support measures for prevention of emergency situations at critical infrastructure facilities.....	277

Секція 6. Психологічне та гуманітарне забезпечення оперативного-рятувальних підрозділів

<i>Алексєєв О.Р., НУЦЗУ</i> Запозичення в галузі термінології пожежогасіння.....	278
<i>Амурова Я.В., ЧПБ ім. Героїв Чорнобиля НУЦЗУ</i> Психологічні особливості реабілітації постраждалих у надзвичайних та екстремальних ситуаціях.....	279
<i>Анацкій Д.Д., НУЦЗУ</i> Особливості повоєнної соціальної адаптації українських військовослужбовців.....	280
<i>Бабенко М.О., ЧПБ ім. Героїв Чорнобиля НУЦЗУ</i> Механізми та особистісні детермінанти професійної самореалізації.....	281
<i>Барміна С.О., ЧПБ ім. Героїв Чорнобиля НУЦЗУ</i> Особливості психопрофілактики професійного вигорання пожежних-рятувальників.....	282