НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

Крім того, подальшого розвитку потребують методи синергетичного управління інформаційною безпекою, спрямовані на використання внутрішніх механізмів самоорганізації віртуальних спільнот. Йдеться про формування умов, за яких деструктивні інформаційні впливи втрачають здатність до масштабування, а система повертається до відносно стійкого стану без застосування надмірних адміністративних або репресивних заходів. У поєднанні з сучасними інструментами аналізу природної мови, мережевої аналітики та елементами штучного інтелекту така методологія може стати основою для побудови ефективних систем забезпечення інформаційної безпеки держави в умовах тривалої війни.

Список використаних джерел

1. Грищук Р., Молодецька-Гринчук К. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах // Захист інформації. – 2017. – Т. 19, № 4 (жовтень–грудень). – С. 254–262. – DOI: 10.18372/2410-7840.19.12204.
2. Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. – Київ : Інтертехнологія, 2009. – 164 с.

Ключові слова: інформаційна безпека держави, соціальні інтернет-сервіси, дезінформація, інформаційно-психологічний вплив.
Keywords: state information security, social internet services, disinformation, information and psychological influence.

A REVIEW ON MANY-VALUED LOGIC: A NOVEL PARADIGM FOR INFORMATION SECURITY

Aboobacker P
Govt.Engineering College, Palakkad, India
Department of Mathematics, Ph.D., Assistant Professor

1. Introduction. In the modern world, technology is changing at an astounding rate. We are more inventive, efficient, and connected than ever. Although this digital revolution has opened up a lot of possibilities, it has also increased risk and complexity. This scenario includes two phases: the incredible opportunity the digital world offers us and the significant challenges we must all overcome to realize that potential.

Modern advancement is built upon connectivity. Cybersecurity is not an obstacle to innovation; rather, it is a crucial enabler that permits us to safely seize new opportunities. The Internet has become the fastest-growing daily infrastructure. Many current technological advancements are transforming society. However, these new

technologies often lack adequate safeguards for personal data, leading to an increase in cybercrimes.

Cybersecurity is the silent, foundational infrastructure for all digital advancement. The digital world relies entirely on this trust and safety; without it, progress stops. The core challenge is simple: as connectivity increases opportunities, it simultaneously expands vulnerabilities, requiring a stronger security foundation to support a more complex world.

2. Cryptography and Cyber security. The fields of communication and cybersecurity are inherently connected. The goal of cybersecurity is to safeguard communication systems and the information they carry, while robust communication is essential for creating, maintaining, and addressing security risks. Strong secure communication is required by the fast-growing interconnection of the entire universe.

Cryptography, the study and application of methods for safe communication and data security against adversaries, is one of the solutions against exploitation in this setting. Encryption is the process of employing mathematical ideas to convert readable data (plaintext) into an unintelligible format (ciphertext) that can only be decoded by the intended recipients. Encryption is an essential and crucial feature of cybersecurity, mainly because it makes sure that data is unreadable even if it is accessed by unauthorized people. It supports a number of important security concepts, such as integrity, confidentiality, and authentication. While cryptography focuses on security, cryptanalysis addresses attack defensive mechanisms.

3. Moving Beyond Binary Choices. The fundamental problem and principle of contemporary cybersecurity research is that current security models are frequently inadequate against changing threats, calling for creative, multi-layered solutions and the creation of new paradigms that go beyond conventional methods. One approach involves moving beyond traditional binary systems to develop methods and systems based on many-valued logic, (MVL) which offers a potential foundation for creating novel and enhanced cryptographic algorithms. Unlike classical two-valued logic—where a statement is strictly true (1) or false (0)—MVL systems incorporate additional truth values (ternary, quaternary, fuzzy logic etc.). This expanded framework provides the capacity to effectively model uncertainty, imprecision, and more complex relationships within computational and security systems.

Benefits of Many-Valued Logic in Cryptography:

– **Compact data representation:** Many-valued logic systems store and analyze more **information per unit**. For instance, with equivalent hardware or the same digit count, a ternary system holds more information per trit than a binary system due to its inherently higher data representation density. This dense processing capability allows custom hardware implementations to potentially achieve better performance while consuming less power.

– **Complex Algorithms with potential:** Incorporating many-valued functions into cryptographic primitives significantly increases their complexity, enhancing security. This approach is fundamental for designing robust components as it elevates the difficulty of solving the underlying mathematical problems faced by attackers.

– **Advanced Algorithmic Methodologies and Optimized Performance:** By implementing MVL number systems like residue and redundant systems, arithmetic operations can be speed up by reducing or eliminating the carry propagation, a key benefit for resource-constrained environments. This capability also facilitates the development of novel, high-quality algorithms. These new algorithms leverage unique properties to offer better statistical parameters, including enhanced nonlinearity and non-correlation than some existing binary based algorithms.

– **Hardware Optimization:** MVL allows designers to reduce both the transistor count and the number of physical connections, which results in Compact, performance-optimized devices.

Disadvantages of Many-Valued Logic in Cryptography:

– **Incompatibility with Binary Infrastructure:** Since most existing computer infrastructure operates exclusively on binary logic, integrating MVL algorithms requires custom hardware or complex software adaptation. This leads to significant difficulty to both the design process and ongoing management.

– **Limited Maturity and Resources:** Compared to classical binary cryptography, the field of MVL cryptography is less developed and lacks standardized protocols. The limited availability of existing research and specialized expertise creates significant hurdles for both development and testing.

– **The changing threat landscape and Limited Research:** The adoption of new logical approaches and nascent circuit systems introduces the risk of novel, previously unstudied vulnerabilities that could be exploited by malicious actors. Furthermore, the limited research into cryptanalysis methods specifically targeting MVL systems makes it challenging to thoroughly evaluate and guarantee the long-term security of these new algorithms compared to established, battle-tested binary ones.

Conclusion. The digital revolution offers extensive opportunities but necessitates a strong security basis as increased connectivity also broadens vulnerabilities. Cryptography is crucial for securing communication and protecting data, with many-valued logic (MVL) proposing a shift from binary systems to develop more complex algorithms. This method could enhance hardware efficiency and cryptographic strength, although challenges persist such as incompatibility with current binary systems, lack of standards, and potential unstudied vulnerabilities. Therefore, despite its promise for future security progress, practical obstacles must be resolved before MVL can be widely adopted.

References:

1. Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. Journal of Cybersecurity, 7(1), tyab005.
2. Stallings, W. Cryptography and Network Security - Principles and Practice.
3. I F. Volynets-Velikorodov and M. S. Klimash. Prospects for the Application of Many-Valued Logic Functions in Cryptography Proceedings of the 2018 IEEE 4th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD).

Ключові слова: кібербезпека, криптографія, багатозначна логіка.
Keywords: cybersecurity, cryptography, many-valued logic.

МЕТОДИ ТА РИЗИКИ ПОБУДОВИ СИСТЕМ З END-TO-END ШИФРУВАННЯМ

Вінковська Ірина

Національний університет «Одеська політехніка»,
старший викладач кафедри кібербезпеки та програмного забезпечення

Чебаненко Олег

Національний університет «Одеська політехніка»,
студент кафедри кібербезпеки та програмного забезпечення

Вступ. Сучасні інформаційні технології забезпечують швидкий обмін даними між користувачами через різноманітні месенджери (Telegram, WhatsApp, Signal тощо). Проте зростання кількості кіберзагроз робить актуальною проблему забезпечення конфіденційності та цілісності повідомлень. Більшість популярних месенджерів використовують власні протоколи шифрування, але їхній вихідний код або архітектура не завжди відкриті для аудиту, що створює ризики втрати контролю над безпекою даних.

У зв'язку з цим постає завдання створення відкритих програмних рішень, які реалізують принцип end-to-end шифрування (E2EE) – коли лише відправник і отримувач мають доступ до змісту повідомлень, а сервер виконує лише роль транспортного посередника.

Мета: Проаналізувати сучасні підходи до реалізації end-to-end шифрування в месенджерах та визначити напрями створення програмного застосунку, який забезпечить конфіденційність, цілісність і автентичність повідомлень під час обміну даними між користувачами.

Проблематика захищеного обміну повідомленнями

Передача даних у мережах часто супроводжується ризиками несанкціонованого доступу, підміни або перехоплення повідомлень.

ЗМІСТ