https://www.securitymagazine.com/articles/92415-verizon-2020-data-breach-report-money-still-makes-the-cyber-crime-world-go-round

2. Global Threat Landscape Report [Електронний ресурс]. – Режим доступу: https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/Threat-Report-H1–2020.pdf

**Ключові слова:** Кібербезпека, кіберзлочинність, кібератака, порушення даних.

**Ключевые слова:** кибербезопасность, киберпреступность, кибератака, нарушение данных.

**Keywords:** cybersecurity, cybercrime, cyberattack, data breach

***Онацький Олексій Віталійович***
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки та інформаційних технологій,
кандидат технічних наук, доцент

***Красношлик Олександр Юрійович***
Національний університет «Одеська юридична академія»,
студент 3 курсу спеціальності 125 – Кібербезпека

## ПРОТОКОЛ АВТЕНТИФІКАЦІЇ НА ОСНОВІ АСИМЕТРИЧНОГО АЛГОРИТМУ ШИФРУВАННЯ

Автентифікація – це процедура перевірки автентичності суб'єкта котрий входить в систему та пред'являє свій ідентифікатор. Основним міжнародним стандартом з криптографічних протоколів автентифікації є стандарт Міжнародної організації зі стандартизації та Міжнародної електротехнічної комісії ISO/IEC9798 – Information technology – Security techniques – Entity authentication, що складається з шести частин [1]:

– ISO/IEC9798–1:2010 Part 1: General;

– ISO/IEC9798–2:2019 Part 2: Mechanisms using authenticated encryption;

– ISO/IEC9798–3:2019 Part 3: Mechanisms using digital signature techniques;

– ISO/IEC9798–4:1999 Part 4: Mechanisms using a cryptographic check function;

– ISO/IEC9798–5:2009 Part 5: Mechanisms using zero-knowledge techniques;

– ISO/IEC9798–6:2010 Part 6: Mechanisms using manual data transfer.

На основі проведеного аналізу стандартів ISO/IEC9798 побудована загальна схема класифікації криптографічних протоколів автентифікації і ідентифікації, яку представлено на рис. 1.

Протоколи автентифікації «запит-відповідь» з використанням асиметричних криптосистем можна розділити на дві групи: протоколи з використанням електронного цифрового підпису та протоколи з використанням криптосистем з відкритим ключем [2]. В роботі запропонований протокол взаємної автентифікації на основі асиметричного алгоритму шифрування RSA.

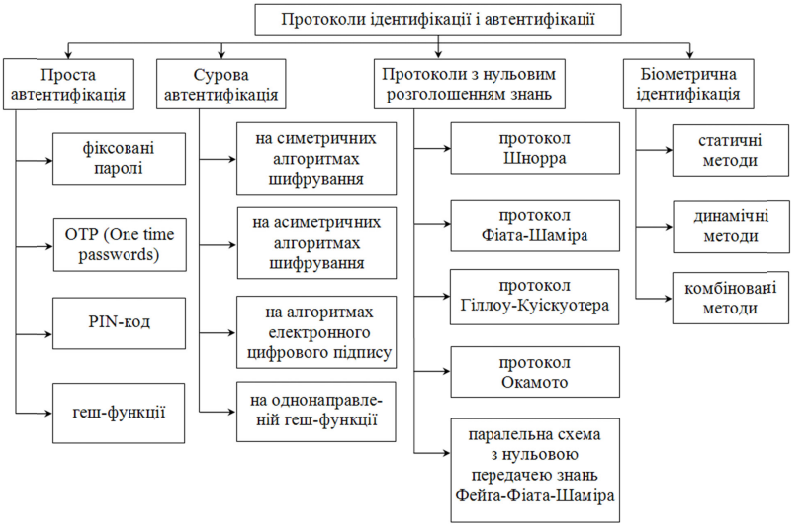


**Рис. 1. Загальна схема класифікації протоколів автентифікації і ідентифікації**

Криптосистема RSA [3; 4] одна з широко використовуваних криптосистем з відкритим ключем. Криптограма обчислюється за правилом $C \equiv M^e \pmod{n}$, де $n$ – добуток двох великих простих чисел $p$ і $q$, $e$ – ключ зашифровування (відкритий ключ), $M$ – повідомлення. Розшифрування виконується за правилом $M \equiv C^d \pmod{n}$, де $d$ – ключ розшифрування (секретний ключ), $C$ – шифртекст (криптограма). Ключова пара $(e, d)$ пов'язана між собою рівнянням $ed \equiv 1 \pmod{\varphi(n)}$, де $\varphi(n)$ – функція Ейлера $\varphi(n) = (p - 1)(q - 1)$. Пара чисел $(n, e)$ робиться відкритим ключем, числа $d$, $p$, $q$ – секретними.

Реалізація протоколу взаємної автентифікації на основі асиметричного алгоритму шифрування RSA представлений на рис. 2, де $e_a$, $e_b$ – відкрити ключі; $d_a$, $d_b$ – секретні ключі; $ID_a$, $ID_b$ – ідентифікатори; $r_a$, $r_b$ – випадкові числа абонентів $A$ та $B$. Деталі реалізації протоколу представлені на рис. 2 в виді трьох кроків. Взаємна автентифікація абонентів $A$ та $B$ виконується після кожного кроку перевірної рівності отриманих значень.

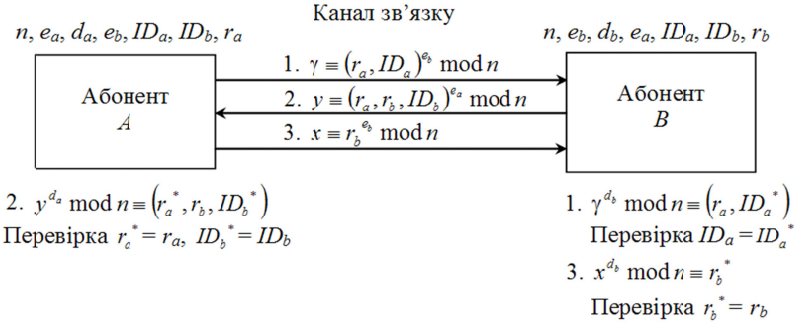


**Рис. 2. Протокол взаємної автентифікації на основі алгоритму RSA**

Однак для правильної роботи протоколу обов'язково використовувати ідентифікатори сторін в іншому випадку можливо атака «людина по середині» (man in the middle – MITM) [5; 6],

приклад реалізації атаки MITM представлена на рис. 3. Крім того можлива атака при використанні загального модуля якщо значення ($r_a$, $ID_a$) = ($r_a$, $r_b$, $ID_b$) будуть однакові (сервер – абонент *B* повинен виключити виконання даного рівняння) [3; 4; 6].

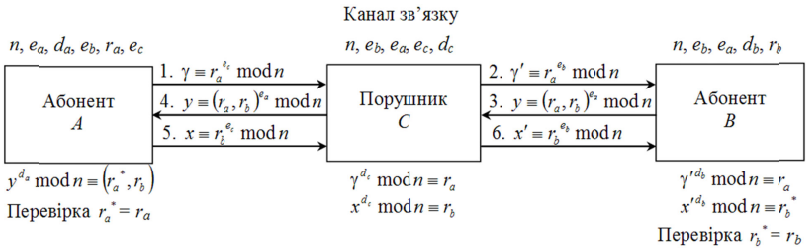


**Рис. 3. Приклад реалізації атаки MITM на протокол взаємної автентифікації (ідентифікатори сторін A та B відсутні)**

В роботі наведено математичне обґрунтування, приклад розрахунку, які показують, що запропонований протокол взаємної автентифікації на основі алгоритму RSA працює коректно та технічно реалізуємо.

**Список використаних джерел:**

1. ISO/IEC 9798. [Електронний ресурс]. – Режим доступу: https://www.iso.org/standards.html

2. Виклик-відповідь (автентифікація). [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Виклик-відповідь_(автентифікація)

3. Бернет С. Криптография. Официальное руководство RSA Security / Бернет С., Пэйн С. – М.: Бином-Пресс, 2002. – 384 с.

4. Bruce Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C / B. Schneier. – Wiley, 2015. – 784 p.

5. Атака посредника. [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Атака_посредника.

6. Menezes A. Handbook of Applied Cryptography / A. Menezes, P. van Oorschot, S. Vanstone. – CRC Press, 1996. – 816 p.

**Ключові слова:** автентифікація, криптографічний протокол, криптосистема з відкритим ключем, шифрування, шифртекст.
**Ключевые слова:** аутентификация, криптографический протокол, криптосистема с открытым ключом, шифрования, шифртекст.
**Keywords:** authentication, cryptographic protocol, public key cryptosystem, encryption, ciphertext.

***Баландіна Наталія Миколаївна***
Національний університет «Одеська юридична академія»,
старший викладач кафедри кібербезпеки

***Василенко Микола Дмитрович***
Національний університет «Одеська юридична академія»,
в.о. завідувача кафедри кібербезпеки,
доктор фізико-математичних наук, доктор юридичних наук,
професор

## ДЕЯКІ НОТАТКИ ЩОДО МАТЕМАТИЧНИХ МОЖЛИВОСТЕЙ В МОДЕЛЮВАННІ ЗАХИСТУ ІНФОРМАЦІЇ

Сучасний стан захисту інформації посприяв розвитку досліджень, які пов'язані з інтелектуалізацією обчислень в галузі підтримки прийняття рішень в кібербезпеці та в захисті інформації в цілому для різних інформаційних систем і технологій. Сьогодні продовжують розроблятися нові методи та моделі для підтримки прийняття рішень щодо вибору і реалізації стратегії захисту інформаційних процесів. В роботі наведено спробу встановлення деяких реальних дій обмежень в питанні математичних можливостей при моделюванні захисту інформації. Очевидно, що моделі захисту інформації являють собою складову частину загального процесу моделювання. І тут моделювання системи полягає у побудові образу системи, адекватного з точністю до цілей моделювання системи, яка проєктується, і в отриманні за допомогою побудованої моделі потрібних характеристик реальної системи з метою побудови захисту. Оскільки інформаційні системи змінюються