МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

ЙОВБАК Андрій Павлович

Алгоритм формування рівнів довіри до методів аутентифікації / Algorithm for Establishing Trust Levels for Authentication Methods

спеціальність: 125 – Кібербезпека

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -21
А.П. Йовбак

Науковий керівник
к.т.н., доцент П.В. Басістий

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2023 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ – 2023

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 – Кібербезпека
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.В.Яцків
«____» _____ 2022 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
ЙОВБАК АНДРІЙ ПАВЛОВИЧ

1. Тема кваліфікаційної роботи:
Алгоритм формування рівнів довіри до методів аутентифікації / Algorithm for Establishing Trust Levels for Authentication Methods
керівник роботи д.т.н., професор М.М. Касянчук
затверджені наказом по університету від «__» _____ 2022 року № _____
2. Строк подання студентом закінченої кваліфікаційної роботи 1 грудня 2023 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
– огляд та аналіз стандартів, що регламентують процеси ідентифікації та аутентифікації;
– проаналізувати механізми односторонньої, взаємної аутентифікації та аутентифікації із залученням третьої сторони;
– розробити класифікацію процесу, систем та засобів аутентифікації;
– розробити модель процесу аутентифікації для дослідження надійності та безпеки її результатів;
– визначити інфраструктуру довіри під час аутентифікації;
– розробити методику формування та оцінювання рівнів довіри до результатів аутентифікації.

5. Перелік графічного матеріалу у роботі:
– послідовність процедури аутентифікації
– графік ймовірності прориву через ешелон оборони;
– приклад допустимих значень відмов у аутентифікації;
– граф станів укрупненої ймовірнісної моделі аутентифікації;
– спрощена схема процесу «Ідентифікація та аутентифікація»;
– граф станів процедури реєстрації.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 8 грудня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз міжнародних і національних нормативних документів стосовно ідентифікації та автентифікації	12.2022 р. – 03.2023 р.	
2	Класифікація та моделювання засобів та процесу формування рівнів довіри при аутентифікації	03.2023 р. – 05.2023 р.	
3	Формування рівнів довіри при аутентифікації суб'єктів доступу	05.2023 р. – 11.2023 р.	

Студент _____ Йовбак А.П.
(підпис)

Керівник роботи _____ к.т.н., доцент П.В.Басістий

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему „Алгоритм формування рівнів довіри до методів аутентифікації” на здобуття освітнього ступеня «Магістр» зі спеціальності 125 „Кібербезпека” освітньо-професійної програми «Кібербезпека» написана обсягом 82 сторінки і містить 12 ілюстрацій, 7 таблиць, 1 додаток та 31 джерело за переліком посилань.

Метою випускної кваліфікаційної роботи є розробка алгоритмів для формування рівнів довіри до методів аутентифікації..

Методи дослідження. Методи моделювання, методи аутентифікації, методи формування критеріїв оцінювання.

Результати дослідження. Здійснено огляд та аналіз нормативно-правових документів, які регламентують процеси ідентифікації та аутентифікації, що дозволило розробити методику формування рівнів довіри. На основі запропонованої методики розроблено класифікацію засобів та систем автентифікації суб'єктів доступу, що дозволило змоделювати процеси аутентифікації для дослідження надійності та безпеки її результатів. На основі основних характеристик процесу аутентифікації суб'єктів доступу розроблено інфраструктуру довіри під час аутентифікації, що дозволило оцінити рівні довіри до результатів аутентифікації. Розроблено алгоритми для формування рівнів довіри до методів аутентифікації.

Результати роботи можуть успішно застосовуватися для формування рівнів довіри до методів аутентифікації.

КЛЮЧОВІ СЛОВА: РІВЕНЬ ДОВІРИ, АУТЕНТИФІКАЦІЯ, ІДЕНТИФІКАЦІЯ, СУБ’ЄКТ ДОСТУПУ, БЕЗПЕКА.

ABSTRACT

The graduate work on the topic „Algorithm for Establishing Trust Levels for Authentication Methods” for Master’s degree on speciality 125 "Cybersecurity " is written on 82 pages and contains 12 illustrations, 7 tables, 1 suplement and 31 references.

The aim of graduate work is the development algorithms for forming levels of trust in authentication methods.

Research methods. Modeling methods, authentication methods, methods of forming evaluation criteria.

Results of the study. A review and analysis of legal documents regulating identification and authentication processes was carried out, which made it possible to develop a methodology for the formation of trust levels. On the basis of the proposed methodology, a classification of means and systems of authentication of access subjects was developed, which made it possible to simulate authentication processes to study the reliability and security of its results. On the basis of the main characteristics of the authentication process of access subjects, a trust infrastructure during authentication was developed, which made it possible to assess the level of trust in the authentication results. Algorithms have been developed for the formation of levels of trust in authentication methods.

The results of the work can be successfully applied to form levels of trust in authentication methods.

Keywords: TRUST LEVEL, AUTHENTICATION, IDENTIFICATION, SUBJECT ACCESS, SECURITY.

ЗМІСТ

ВСТУП

Зі зростанням інформатизації суспільства та збільшенням кількості інформаційних систем (ІС) [1-2] виникла потреба в управлінні доступом користувачів до інформаційних ресурсів [3-4]. Це включає процеси ідентифікації та аутентифікації користувачів через інформаційні системи [5-7]. Аутентифікація особливо важлива в умовах недостатньої довіри до ідентифікації, зокрема при віддаленому доступі або загрозах кібератак [8-9].

Сучасний світ стикається зі зростаючими загрозами кібербезпеки, коли ІС можуть бути атаковані з метою несанкціонованого доступу до інформаційних ресурсів [10-12]. Питання довіри до результатів ідентифікації та аутентифікації користувачів стає ключовим для всіх ІС [13-14]. Для зменшення ризиків і підвищення рівня довіри до взаємодії між суб'єктами та об'єктами доступу, необхідно використовувати науково обґрунтовані методи, механізми та інструменти ідентифікації та аутентифікації. Це становить важливу частину систем управління доступом, що є необхідною складовою ІС.

Завдання управління ідентифікацією та аутентифікацією для інформаційних систем із обмеженим доступом важливі [15-17]. Однією з основних функцій управління доступом є авторизація користувачів і визначення їхнього права на доступ.

На сьогодні відзначається відставання у регулюванні ідентифікації та аутентифікації. Міжнародні стандарти [18-20] в цій галузі постійно змінюються, що призводить до проблем у створенні нормативно-правової бази і обмежує якість національної технічної бази, такої як стандарти, методики, інструкції тощо, а також методи, протоколи та технології.

Це веде до випадкового вибору методів ідентифікації та аутентифікації власниками інформаційних систем та підвищує їхню вразливість до атак та несанкціонованого доступу. Необхідно поліпшити нормативно-правову базу та створити методичні рекомендації для забезпечення безпеки і надійності ідентифікації та аутентифікації в інформаційних системах.

У розвитку ІС з великою кількістю користувачів виникають важливі питання, які потребують досліджень та розробки ієрархії довіри до результатів ідентифікації та аутентифікації [21-22]. Різноманітність технічних рішень та відсутність чіткої нормативної бази роблять цей процес складним, але дуже актуальним у світі інформаційних систем.

У нормативно-правовому полі необхідно розробити механізми надійного доступу до державних інформаційних систем (ДІС) з певним рівнем довіри до аутентифікації користувачів. Для цього потрібно провести аналітичні дослідження та розробити теоретичні основи методології. Це важлива проблема, оскільки довіра до результатів ідентифікації та аутентифікації є ключовим фактором у віддаленій електронній взаємодії.

Проте, досі не існує науково обґрунтованих підходів та методик для комплексного аналізу на науковій основі. Таким чином, проблема створення ієрархії довіри до ідентифікації та аутентифікації є актуальною та потребує подальших наукових досліджень.

Розробка та модернізація існуючих методів, моделей та алгоритмів оцінки довіри до ідентифікації та аутентифікації допоможуть сформулювати теоретичне обґрунтування для розробки стандартів, рекомендацій та вимог до процесів та систем ідентифікації та аутентифікації суб'єктів доступу в існуючих та проектованих інформаційних системах.

Мета роботи. Метою роботи є розробка алгоритмів для формування рівнів довіри до методів аутентифікації.

Для вирішення поставленої мети вирішуються наступні **завдання**:

– огляд та аналіз стандартів, що регламентують процеси ідентифікації та аутентифікації;

– проаналізувати механізми односторонньої, взаємної аутентифікації та аутентифікації із залученням третьої сторони;

– розробити класифікацію процесу, систем та засобів аутентифікації;

– розробити модель процесу аутентифікації для дослідження надійності та безпеки її результатів;

– визначити інфраструктуру довіри під час аутентифікації;

– розробити методику формування та оцінювання рівнів довіри до результатів аутентифікації.

Об’єкт дослідження. Процес аутентифікації суб'єктів доступу.

Предмет дослідження. Методи і засоби для аутентифікації суб'єктів доступу.

Методи дослідження. Методи моделювання, методи аутентифікації, методи формування критеріїв оцінювання.

Наукова новизна одержаних результатів.

1. Здійснено огляд та аналіз нормативно-правових документів, які регламентують процеси ідентифікації та аутентифікації, що дозволило розробити методику формування рівнів довіри.

2. На основі запропонованої методики розроблено класифікацію засобів та систем автентифікації суб'єктів доступу, що дозволило змоделювати процеси аутентифікації для дослідження надійності та безпеки її результатів.

3. На основі основних характеристик процесу аутентифікації суб'єктів доступу розроблено інфраструктуру довіри під час аутентифікації, що дозволило оцінити рівні довіри до результатів аутентифікації.

Практичне значення отриманих результатів. Розроблено алгоритми для формування рівнів довіри до методів аутентифікації.

Публікації та апробація КР.

1. Йовбак А.П., Марків А.П., Касянчук М.В. Огляд сучасних міжнародних стандартів для регламентації процесів аутентифікації. Збірник матеріалів науково - практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2023), Тернопіль, 2023. С.136-138 [23].

2. Йовбак А.П., Осадчук О.Й., Касянчук В.М. Моделювання процесу аутентифікації для дослідження її надійності та безпеки інформації. Матеріали науково-практичного симпозіуму «Захист інформації». Тернопіль, 2023. С.78-82 [24].

1 АНАЛІЗ МІЖНАРОДНИХ І НАЦІОНАЛЬНИХ НОРМАТИВНИХ ДОКУМЕНТІВ СТОСОВНО ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

1.1 Огляд стандартів, що регламентують ідентифікацію та аутентифікацію

Основи безпеки взаємодії відкритих систем, зокрема при управлінні доступом користувачів викладено у роботах спеціалістів відомих науково-дослідних інститутів National Institute of Standards and Technology (NIST, США) та British Standards Institution (BSI, Велика Британія) [25-27].

Історія розроблення стандартів з ідентифікації та автентифікації тісно пов'язана з історією розвитку інформаційних технологій і особливо технологій віддаленої електронної взаємодії. Інтенсивне зростання відкритих систем масового електронного обслуговування (e-Banking, e-Commerce, e-Government, e-Health та інших складових інформатизації суспільства) зажадало створення сервісів безпеки, що забезпечують прийнятний рівень ризиків використання інформаційних систем. Одним із найскладніших, але необхідних елементів інформаційної системи є сервіс автентифікації - підтвердження автентичності пред'явлених заявником ідентифікаторів і доказу приналежності конкретному суб'єкту. Цей факт знайшов відображення в системі міжнародних стандартів. Нормативних документів щодо автентифікації в кількісному відношенні набагато більше, ніж щодо ідентифікації, а історія їх набагато багатша і триває вже понад 30 років.

На рисунку 1.1 наведено аналіз хронології розвитку стандартів з ідентифікації та автентифікації з урахуванням їхнього змісту, який показав наявність певних тенденцій.

В 1988 р. відбулося прийняття першої версії рекомендацій X.509 Міжнародного союзу електрозв'язку. Необхідно зазначити, що з першої версії цього документа ITU-T Rec.X.509 (08/1988) до третьої ITU-T Rec.X.509 (08/1997) , виданої 1997 р., рекомендація мала назву "Директорія: основи автентифікації"; в останніх версіях, наприклад, 2012 і 2015 років, у назві залишається "Директорія: основи PKI та атрибути сертифікатів" [28-29]. Наведено два види

аутентифікації: проста, із застосуванням як аутентифікатора пароля, і сувора, із застосуванням криптографічних функцій [30-31].

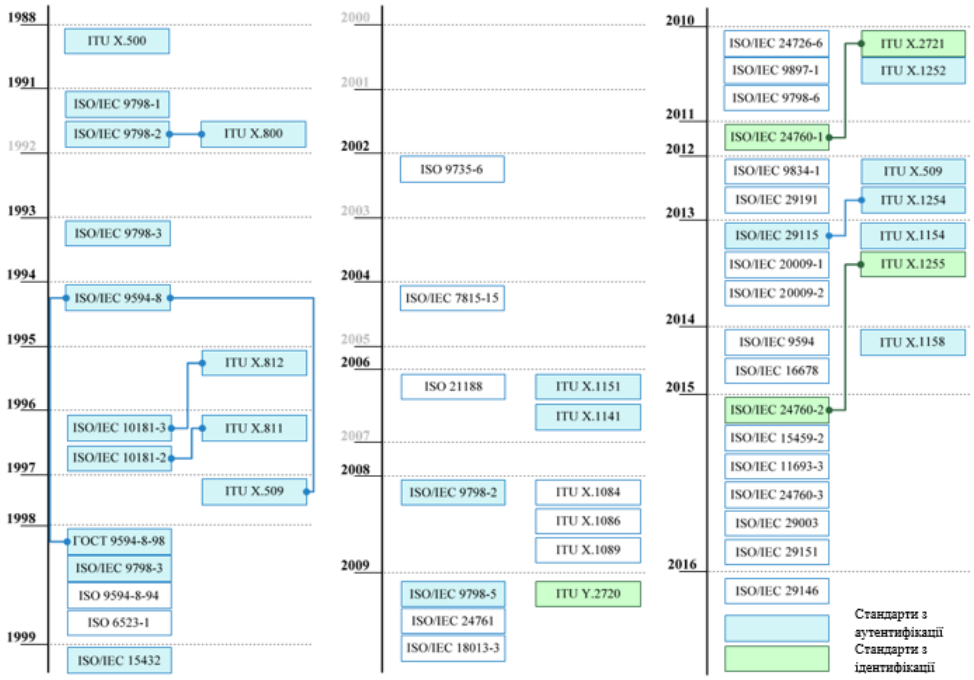

Рисунок 1.1 - Хронологія розвитку міжнародних стандартів з ідентифікації та автентифікації

В 1991 р. одним із перших стандартів з автентифікації користувачів відкритих систем, розроблених ISO, став стандарт "Загальна модель механізмів автентифікації об'єктів". Майже одночасно з ним було опубліковано стандарт з архітектури безпеки для взаємозв'язку відкритих систем, технічно узгоджений із рекомендацією ITU Rec.X.800, у якому докладно розглянуто базові послуги безпеки, насамперед автентифікацію, на рівнях еталонної моделі взаємодії відкритих систем (OSI). Зауважимо, що стандарт ISO/IEC 9798-1:1991, який спочатку складався з трьох частин (перші частини вийшли в 1991 р., третя частина - у 1993 р.), перевидавався кілька разів. Наприклад, частину 2 вперше було опубліковано в 1991 р., вдруге - у 1996 р., востаннє - у 2018 р.

В 1996 р. до числа перших стандартів із забезпечення безпеки процесів автентифікації, тісно пов'язаних із побудовою систем забезпечення довіри при віддаленій електронній взаємодії, почав належати ISO/IEC 10181-2. Текст

стандарту повністю ідентичний випущеним того ж року рекомендаціям ITU-T Rec.X.811. Ці рекомендації спиралися на стандарт Міжнародного союзу електрозв'язку щодо загальної безпеки взаємодії відкритих систем.

В 1997 р. вийшла друком повністю переглянута версія стандарту ITU-T Rec.X.509, пов'язаного (практично ідентичного, відмінність тільки в описі технічних подробиць у стандарті МСЕ) з розглянутою вище восьмою частиною стандарту ISO/IEC 9594-8-94. Обидва пов'язані стандарти називаються "Основи аутентифікації". Описано та специфіковано просту та сувору автентифікацію із застосуванням асиметричної криптографії. Представлено основні сервіси безпеки на базі інфраструктури відкритих ключів: автентифікація джерела даних і взаємна автентифікація, управління доступом, конфіденційність даних, цілісність і невідповідність. Також визначено основні механізми, що застосовуються в зазначених сервісах: проста і сувора автентифікація, шифрування і цілісність даних, електронний підпис.

В 1998 р. опубліковано перероблену третю частину стандарту ISO/IEC 9798, присвячену застосуванню криптографічних алгоритмів цифрового підпису для автентифікації об'єктів і суб'єктів. Стандарт містить чотири механізми автентифікації: два для односторонньої автентифікації об'єкта і два для взаємної автентифікації. Розглянуто можливості застосування таких криптографічних алгоритмів: симетричних алгоритмів, цифрового підпису, криптографічної функції перевірки та механізму з нульовим знанням.

В 2009 р. опубліковано стандарт ITU-T Rec.Y.2720, що узагальнює напрацювання багатьох рекомендацій, зокрема ITU-T Rec.X.1151, ITU-T Rec.X.1141, для управління ідентифікацією об'єктів і суб'єктів у мережах нового покоління. У системі ISO/IEC перша частина аналогічного призначення стандарту з'явиться лише в 2011 р. (ISO/IEC 24760-1). Положення стандарту ISO розглядають ті самі категорії, що й стандарт ITU-T Rec.Y.2721 (2010) .

В 2013 р. застосування методів управління ризиками до завдань ідентифікації та автентифікації, а також поява низки робіт NIST. сприяли

створенню першого стандарту ISO за рівнями довіри до автентифікації - ISO/IEC 29115, гармонізованого з ITU-T Rec.X.1254.

В 2015 р. опубліковано стандарт ISO/IEC 24760-2, що відповідає рекомендаціям ITU-T Rec.X.1255 (09/2013), з управління ідентифікацією. Основні положення цих стандартів спираються на стандарти ISO/IEC 24760-1:2011 та ISO/IEC 29115:2013.

Робота з розвитку та оновлення стандартів триває. За останні 5 років кількість щорічно публікованих стандартів з ідентифікації та автентифікації істотно зросла, водночас акцент із загальних принципів розв'язання завдань ідентифікації та автентифікації зміщується в бік прикладного застосування цих процесів у різних галузях (медицина, фінанси, транспорт тощо).

Аналіз кількості стандартів ISO, безпосередньо пов'язаних із розвитком технологій ідентифікації та автентифікації, за роками видання показав, що якщо в період з 1996 по 2008 р. випускали не більше одного стандарту на рік, то в період з 2009 по 2015 р. видавали по 2-3 стандарти. При цьому кількість стандартів, пов'язаних із цифровою ідентифікацією та автентифікацією в різних сферах життєдіяльності (фінанси, транспорт, охорона здоров'я тощо), зростала в арифметичній прогресії. Наприклад, при контекстному запиті на сайті ISO за терміном "authentication" за останні 10 років наводиться 66 стандартів. Стандарти змінювалися не тільки кількісно, а й якісно. Так, якщо в ISO/ IEC 10181-2:1996 було закладено теоретичні засади (учасники обміну, види переданої автентифікаційної інформації, моделі загроз тощо) усіх видів автентифікації, то вже в ISO/МЕК 9798-3:1998 було описано два види автентифікації: простий (із використанням як автентифікатора пароля) та суворий (як автентифікатор застосовують закритий ключ цифрового підпису, відповідний до сертифіката доступу).

Встановлено, що під час розроблення стандартів дотримувалися їхньої спадкоємності та ідентичності. Наприклад, єдиний стандарт з автентифікації ISO/МЕК 9594-8-98 є перекладом стандарту ISO/IEC 9594-8:1994 та одночасно частиною пов'язаного з ним стандарту ITU Rec.X.509.

До найважливіших з погляду регламентації процедур ідентифікації та автентифікації слід віднести стандарти з таблиці 1.1 (пов'язані між собою стандарти розташовані в одному рядку):

– визначають теоретичні засади, базову архітектуру та термінологію в галузі ідентифікації та автентифікації;

– визначають питання, пов'язані з довірою до ідентифікації та автентифікації;

– регламентують процеси управління ідентифікацією та автентифікацією.

Таблиця 1.1 - Відповідність стандартів МСЕ та ISO з ідентифікації та аутентифікації

ITU-T x.800 (1991) Методи захисту. Автентифікація об'єктів. Архітектура безпеки для взаємодії відкритих систем	ISO/IEC 7498-2:1989 Аутентифікація об'єктів. Архітектура безпеки для взаємодії відкритих систем
ITU-T x.509 (1997) Взаємодія відкритих систем. Довідник сертифікатів. Основи автентифікації.	ISO/IEC 9594-8:1998 Взаємозв'язок відкритих систем. Довідник. Частина 8. Основи аутентифікації
ITU-T x.811 (1995) Теоретичні основи аутентифікації	ISO/IEC 10181-2:1996 Основи безпеки для відкритих систем. Частина 2. Основи аутентифікації
ITU-T x.1252 (2010) Базові терміни та визначення в галузі управління ідентифікацією	ISO/IEC 24760-1:2011 Посібник з управління ідентифікацією. Частина 1. Термінологія та поняття
ITU-T x.1254 (2012) Структура гарантії автентифікації об'єкта	ISO/IEC 29115:2013 Структура довіри до автентифікації сутності
ITU-T x.1255 (2013) Структура виявлення інформації з управління ідентифікацією	ISO/IEC 24760-1:2015 Загальні засади управління ідентифікацією. Частина 2. Еталонна архітектура та вимоги

Починаючи з 2009 р. (поява стандарту ISO/IEC 9798-5:2009), поняття "ідентифікація" та "аутентифікація" стали досить близькими. Дійсно, довіра до результатів аутентифікації істотно залежить від коректності проведення

первинної ідентифікації. Завдяки цьому опубліковані останніми роками стандарти дедалі частіше оперують більш загальним поняттям "ідентифікація".

При цьому, на відміну від стандартів з автентифікації, що мають майже столітню історію, розвинені стандарти з ідентифікації з'явилися відносно нещодавно (так, стандарт ITU-T Y.2720 прийнято у 2009 р., решта ще пізніше). Можливою причиною виникнення такої ситуації стала відсутність адекватних математичних моделей ідентифікації, необхідних для розв'язання завдань у широкому діапазоні інформаційних систем, які нерідко налічують десятки мільйонів і більше користувачів.

У стандартах ITU-T Rec.X.1254 (09/2012) та ISO/IEC 29115:2013 на основі аналізу ризиків запропоновано 4 рівні довіри до результатів ідентифікації, вказані у таблиці 1.2.

Таблиця 1.2 – Рівень довіри до результатів ідентифікації

Рівень	Опис	Задача	Засоби контролю
1	2	3	4
Рівень1 – низький	Слабкий ступінь впевненості в заявленій ідентичності	Ідентичність унікальна в рамках контексту	Власне затвердження чи заява
Рівень 2 – середній	Певний ступінь упевненості в заявленій ідентичності	Ідентичність унікальна в рамках контексту, і об'єкт, що володіє ідентичністю, реально існує	Перевірка автентичності ідентичності шляхом використання інформації з авторитетного джерела
Рівень 3 - високий	Високий ступінь упевненості в заявленій ідентичності	Ідентичність є унікальною в рамках контексту, об'єкт реально існує, ідентичність верифікована, ідентичність використовується в інших контекстах	Перевірка автентичності ідентичності шляхом використання інформації з авторитетного джерела + верифікація ідентичності

Продовження таблиці 1.2

1	2	3	4
Рівень 4 - дуже високий	Дуже високий ступінь упевненості в стверджуваній або заявленій ідентичності	Ідентичність унікальна в рамках контексту, об'єкт реально існує, ідентичність верифікована, ідентичність використовується в інших контекстах	Перевірка автентичності ідентичності шляхом використання інформації з достовірного джерела + верифікація ідентичності + особиста присутність об'єкта

На рисунку 1.2 розглянуто механізми автентифікації, визначені в основоположних стандартах ISO/IEC 9594-8:1994 та ISO/IEC 29115:2013, порівняно зі стандартом FIDO, який часто згадують.

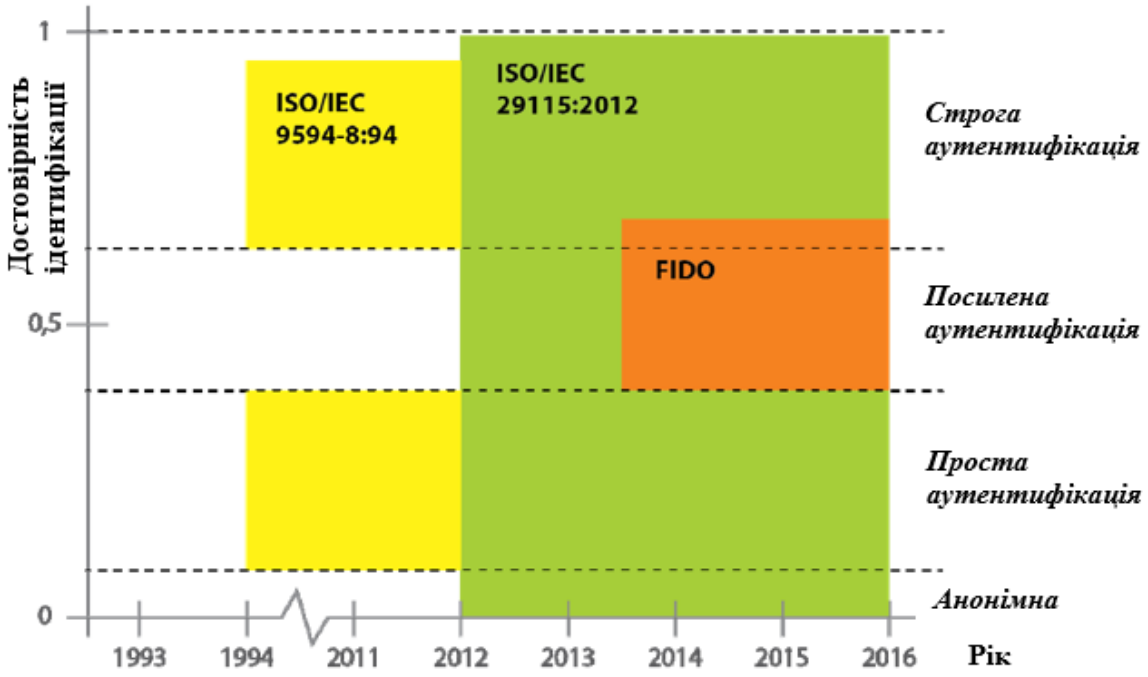

Рисунок 1.2 - Області охоплення стандартами рівнів достовірності аутентифікації

Видно, що, на відміну від ISO/IEC 9594-8:1994, стандарт ISO/IEC 29115:2013 охоплює всі рівні достовірності ідентифікації. Водночас стандарт , хоч і оперує терміном "сувора автентифікація", часто підміняє це поняття

двофакторною автентифікацією, яка може і не бути суворою. Рекомендується, наприклад, використовувати фактор знання та одну з біометричних характеристик користувача (або одразу дві): відбиток пальця, голос тощо, або іншу пару: фактор володіння і поведінкову характеристику. Для фахівця зрозуміло, що всі біометричні характеристики є ідентифікаційною інформацією, тобто інформацією без підтвердження, і їх не можна безпосередньо розглядати як інформацію, що аутентифікує. Будь-яка біометрична характеристика може слугувати лише підтвердженням, наприклад, фактора володіння.

У першій частині ISO/IEC 24760 подано терміни та визначення. Друга частина стандарту - ISO/IEC 24760-2 - містить рекомендації щодо реалізації системи менеджменту ідентифікаційних атрибутів, а також визначає вимоги щодо реалізації загальних принципів менеджменту. Положення частини ISO/IEC 24760-2 застосовні до будь-якої інформаційної системи, в якій обробляється або зберігається інформація ідентифікаційного характеру. Ця частина надає базу для реалізації інших міжнародних стандартів, пов'язаних з опрацюванням ідентифікаційної інформації, і містить два основні розділи: "Еталонна архітектура" і "Вимоги до управління ідентифікаційна інформація (II)". Третя частина стандарту - ISO/IEC 24760-3 - містить настанови щодо менеджменту ідентифікаційної інформації та зниження ризиків стосовно ідентифікаційної інформації. Окремий розділ стандарту присвячено заходам щодо реалізації адекватних заходів, спрямованих на зниження ризиків та усунення наслідків витоків ідентифікаційної інформації, пошкодження та втрати достовірності в рамках її збирання, зберігання, використання, передавання та видалення. У стандарті міститься стислий перелік політик доступу до ідентифікаційної інформації, які розкривають вимогу про необхідність ведення процедур її безпечного менеджменту.

У рекомендаціях ITU-T Y.2720 "Global information infrastructure. Internet protocol aspects and next-generation networks. NGN identity management framework" представлено основи менеджменту ідентифікаційних атрибутів у мережах нового покоління. Головною метою цього документа є опис

структурного підходу до проектування, визначення та реалізації рішень у сфері менеджменту ідентифікаційних атрибутів і сприяння функціональній сумісності в гетерогенному середовищі.

Зіставлення з еталонною архітектурою менеджменту ідентифікаційних атрибутів, визначеною в ISO/IEC 24760, дає змогу зазначити, що в останньому стандарті уявлення про інфраструктуру системи менеджменту ідентифікаційної інформації отримало принциповий розвиток: якщо в Y.2720 інфраструктуру визначали переважно в термінах функцій і можливостей, то в ISO/IEC 24760 вона являє собою взаємопов'язану сукупність суб'єктів, що діють, потоків інформації, сервісів, сховища, рівнів доведення тощо.

1.2 Механізми односторонньої та взаємної аутентифікації

Група стандартів під загальним індексом ISO/IEC 9798 "Information technology - Security techniques - Entity authentication" надає користувачам набір родин протоколів і призначених для автентифікації сутностей (суб'єктів і об'єктів). ISO/IEC 9798 складається з шести частин. У кожній із частин стандарту розглянуто механізми односторонньої та взаємної автентифікації, запропоновано різну суворість їхньої реалізації через введення відповідної кількості ітерацій інформаційного обміну (які називають проходами) відповідними протокольними блоками даних, сформованими на основі застосування того чи іншого криптографічного алгоритму або примітиву.

Механізми суворої аутентифікації реалізуються із застосуванням:

– симетричних криптографічних алгоритмів. У стандарті ISO/IEC 9798-2 розглянуто 6 механізмів і до 4 проходів протокольного обміну);

– електронного підпису та інфраструктури відкритих ключів. У стандарті ISO/IEC 9798-3 розглянуто 10 механізмів і до 7 проходів протокольного обміну;

– забезпечують контрольні функції криптографічних алгоритмів (надійні позначки часів, надійні датчики випадкових чисел). У стандарті ISO/IEC 9798-4 розглянуто 4 механізми і до 3 проходів протокольного обміну;

– початкових "нульових знань". У стандарті ISO/IEC 9798-5 розглянуто 6 механізмів, що базуються на різних криптографічних алгоритмах і алгебраїчних операціях для автентифікації пристроїв, що використовують інформаційні технології.

Стандарт ISO/IEC 9798-6 встановлює 8 механізмів і множинний взаємний обмін.

Розглянемо перші три частини міжнародного стандарту ISO/IEC 9798 як такі, що найбільшою мірою стосуються досліджуваної в дисертації галузі.

Перша частина стандарту ISO/IEC 9798-1 визначає модель автентифікації, загальні вимоги й обмеження для механізмів автентифікації сутності, що використовують засоби захисту. Ці механізми застосовуються для підтвердження, що сутність є тим, що вона про себе заявляє.

Відповідно до узагальненої моделі, зображеної на рисунку 1.3, зовсім не вимагається, щоб будь-який механізм автентифікації містив усі показані сутності та реалізовував обмін даними в усіх зазначених напрямках.

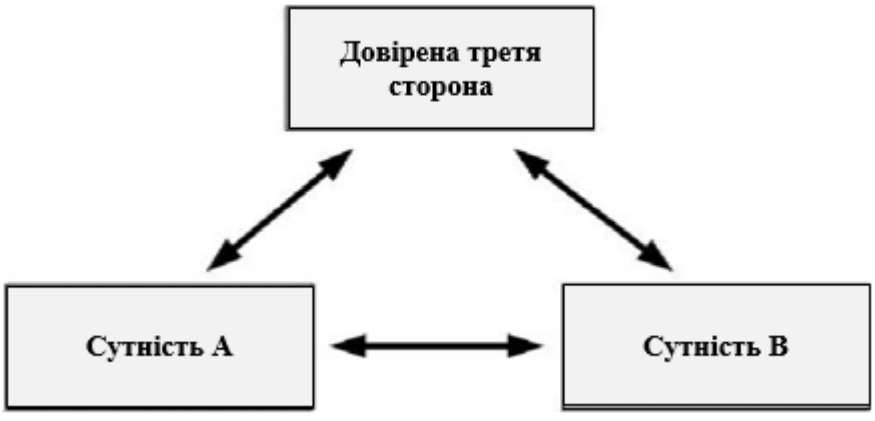

Рисунок 1.3 - Узагальнена модель аутентифікації

Стосовно механізмів автентифікації, визначених в інших частинах ISO/IEC 9798, діють такі положення:

– у разі односторонньої автентифікації сутність А розглядають як заявника, а сутність В - як реєстратора та довірливу сторону (контролера);

– у разі взаємної автентифікації сутності А і В виступають у ролі як заявника, так і контролера.

У межах процесів автентифікації сутності генерують і обмінюються формалізованими повідомленнями - токенами. Інформаційний обмін включає передачу щонайменше одного токена для односторонньої аутентифікації та двох - для взаємної. При цьому може знадобитися додаткова передача для запиту про початок обміну, а також додаткові обміни даними, якщо до процесу аутентифікації залучається довірена третя сторона. Детальний опис цих механізмів і зміст операцій інформаційного обміну в рамках процесу аутентифікації наводиться в наступних частинах ISO/IEC 9798.

Друга частина стандарту ISO/IEC 9798-2 визначає механізми автентифікації сутності, що використовують алгоритми симетричного шифрування. Чотири з цих механізмів забезпечують автентифікацію в межах взаємодії двох сутностей за відсутності довіреної третьої сторони: два механізми призначено для односторонньої автентифікації сутності та два - для взаємної автентифікації двох сутностей. Решта механізмів вимагають наявності довіреної третьої сторони для встановлення спільного секретного ключа і реалізують взаємну й односторонню аутентифікацію сутності.

Механізми, визначені в міжнародному стандарті ISO/IEC 9798-2, використовують параметри, що змінюються в часі, як-от тимчасові мітки, рядкові номери або випадкові числа, щоб запобігати можливості використання актуальної автентифікаційної інформації більше одного разу або після закінчення часу.

Одностороння автентифікація характеризується тим, що автентифікується тільки одна із сутностей. В умовах, коли не задіюється довірена третя сторона і використовуються тимчасові мітки або порядкові номери, для односторонньої автентифікації необхідне виконання протоколу з одним проходом, а якщо

застосовується запитно-відповідний протокол з використанням випадкових чисел, то для односторонньої автентифікації потрібні два проходи.

Взаємна автентифікація характеризується тим, що обидві сутності автентифікують одна одну в процесі взаємодії. В умовах, коли не задіюється довірена третя сторона і використовуються тимчасові мітки або порядкові номери, для взаємної автентифікації необхідне виконання протоколу з двома проходами, а якщо застосовується запит-відповідь протокол з використанням випадкових чисел, то для взаємної автентифікації потрібні три проходи.

1.3 Механізми аутентифікації із залученням третьої сторони

У механізмах аутентифікації із залученою третьою стороною не використовується етап поділу секретного ключа між двома сутностями до початку процесу аутентифікації. Замість цього використовують довірену третю сторону, з якою кожна зі сторін А і В поділяють свій секретний ключ. У межах цих методів одна із сутностей запитує ключ у довіреної третьої сторони.

У третій частині стандарту ISO/IEC 9798-3 визначено методи автентифікації сутності, що використовують електронний підпис і засновані на асиметричних криптографічних алгоритмах. При цьому електронний підпис необхідний для перевірки автентичності сутності. Для запобігання можливості застосування коректної аутентифікаційної інформації після закінчення відведеного часу використовують параметри, що змінюються в часі (мітки часу, порядкові номери, випадкові числа).

У разі використання міток часу або порядкових номерів для односторонньої аутентифікації потрібне виконання одного проходу, а для взаємної - два. Якщо застосовується запитно-відповідний протокол із використанням випадкових чисел, то для односторонньої автентифікації потрібні два проходи, а для взаємної - три або чотири залежно від застосовуваного методу.

У документі визначено десять механізмів. Перші п'ять механізмів не передбачають залучення довіреної третьої сторони, яка має бути доступною в режимі онлайн, а група механізмів, що залишилися, передбачає її наявність. Обидві групи включають по два механізми односторонньої автентифікації і три механізми взаємної автентифікації.

У методах автентифікації, визначених у документі, сутність, що автентифікується, підтверджує свою справжність, демонструючи знання свого секретного ключа підпису. Це досягається тим, що сутність використовує секретний ключ для підпису певних повідомлень. Підпис може бути перевірений будь-якою стороною з використанням відкритого ключа перевірки.

Міжнародний стандарт ISO/IEC 10181-2 / ITU-T X.811 «Information technology – Open systems interconnection – Security frameworks for open systems: Authentication framework» присвячений застосуванню сервісів безпеки в середовищі "відкритих" систем, до числа яких, зокрема, віднесено бази даних, розподілені додатки, системи відкритого розподіленого оброблення та модель взаємодії відкритих систем. Стандарт визначає основні концепції автентифікації, можливі класи механізмів автентифікації, сервіси виділених класів, функціональні вимоги для протоколів з підтримки виділених класів, загальні вимоги менеджменту для автентифікації. Деякі процедури, описані в рамках цього стандарту, забезпечують безпеку за допомогою застосування криптографічних методів. При цьому визначено такі типи аутентифікаційної інформації:

- аутентифікаційна інформація (AI) рівня обміну (exchange authentication information);
- AI рівня пред'явлення (claim authentication information);
- I рівня контролю (verification authentication information).

У деяких випадках з метою проведення процедури обміну AI заявнику може знадобитися звернення до довіреної третьої сторони (ДТС). У свою чергу і контролер теж може звернутися до ДТС з метою проведення процедури обміну

AI. У таких випадках ДТС може зберігати AI рівня контролю, що стосується сторони, яка взаємодіє.

AI рівня пред'явлення належить до допоміжної та використовується під час формування аутентифікаційної інформації рівня обміну, необхідної для аутентифікації одного з учасників інформаційної взаємодії. AI рівня контролю використовується для перевірки автентичності, заявленої в рамках AI рівня обміну. AI рівня обміну являє собою інформацію, якою обмінюються заявник і контролер протягом процедури автентифікації суб'єкта.

Механізми аутентифікації можуть бути схильні до впливу атак, реалізація яких знижує їхню ефективність. У міжнародному стандарті ISO/IEC 10181-2 / ITU-T X.811 розглядаються механізми автентифікації для проведення процедури автентифікації у фазі передачі даних. Ці механізми класифікуються залежно від загроз, до блокування яких вони стійкі.

Міжнародний стандарт ISO/IEC 9594-8 / ITU-T X.509 "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute cer- tificate frameworks [Directory authentication]" розроблено для спрощення взаємовідносин систем обробки інформації з метою забезпечення служб каталогу (di- rectory services). При цьому перша версія цього стандарту мала назву "Основи аутентифікації". Як правило, термін "каталог" використовується для зазначення організованого набору інформації або файлів, які можуть запитуватися для отримання конкретної інформації. У ширшому сенсі в контексті стандартизації безпеки та електрозв'язку термін "каталог" позначає сховище інформації, яке надає послуги для спрощення зв'язку та обміну інформацією між об'єктами, людьми, терміналами, списками розсилки тощо.

Під час роботи в рамках каталогу в центрі уваги постійно перебуває ЗІ (захист інформації), яка є головною метою управління підтвердженням автентичності. ЗІ каталогу - це головним чином питання захисту від несанкціонованого розкриття ПДн, але вона також містить у собі забезпечення цілісності даних і захист активів, що представляються цими даними.

Каталог може допускати анонімний доступ до деякої незначної інформації. Однак для отримання доступу до більш важливих даних потрібен певний рівень аутентифікації користувачів. У документі пропонується кілька рівнів аутентифікації:

- тільки ім'я;
- ім'я та пароль, який передається у вигляді відкритого тексту;
- ім'я та захищений пароль, тобто пароль, який хешується з будь-якою додатковою інформацією для гарантії, що буде виявлено будь-яку спробу отримати доступ до каталогу шляхом відтворення хешованого значення;
- надійна аутентифікація, за якої відправник підписує певну інформацію за допомогою цифрового підпису. Підписана інформація містить ім'я одержувача та додаткову інформацію, яка також дає змогу виявляти спроби входу.

Для різного типу користувачів, які мають доступ, потрібні різні рівні захисту. Рівень аутентифікації користувача також впливає на права доступу для цього користувача. Права доступу користувача або групи користувачів залежать від рівня довіри до аутентифікації. Отримання важливої інформації або оновлення записів зазвичай вимагає вищого рівня автентифікації, ніж отримання менш важливої інформації.

Інфраструктура відкритих ключів спрощує управління відкритим ключем для надання послуг автентифікації, шифрування, цілісності та збереження інформації. Фундаментальною технологією для інфраструктури з відкритим ключем є шифрування з відкритим ключем.

Міжнародний стандарт ISO/IEC 9594-8 / ITU-T X.509 - це стандарт для суворої аутентифікації, заснованої на сертифікатах відкритого ключа. На додаток до визначення структури автентифікації для інфраструктури відкритих ключів міжнародний стандарт описує інфраструктуру управління повноваженнями, яка використовується для перевірки прав і повноважень користувачів у контексті надійної авторизації. У стандарті визначено інфраструктуру відкритих ключів, до якої входить специфікація об'єктів даних,

що використовуються для представлення як самих сертифікатів, так і сповіщень про анулювання виданих сертифікатів, які більше не повинні визнаватися дійсними. У стандарті ISO/IEC 9594-8 / ITU-T X.509 установлено структуру і правила атрибутних сертифікатів, до яких включено специфікацію об'єктів даних, що використовуються для подання як самих сертифікатів, так і повідомлень про анулювання виданих сертифікатів. У ньому визначено інформаційні об'єкти для зберігання об'єктів інфраструктури відкритих ключів та інфраструктури управління повноваженнями в каталозі, а також для порівняння представлених значень зі значеннями, що зберігаються. Крім того, у документі визначено структуру для надання каталогом послуг автентифікації його користувачам.

2 КЛАСИФІКАЦІЯ ТА МОДЕЛЮВАННЯ ЗАСОБІВ ТА ПРОЦЕСУ ФОРМУВАННЯ РІВНІВ ДОВІРИ ПРИ АУТЕНТИФІКАЦІЇ

2.1 Принципи формування критеріїв класифікації

Аналіз багаторічної практики створення та експлуатації систем автентифікації показує, що вони відносяться до класу інтелектуальних систем, опис яких через розмаїття застосованих технологій, механізмів і засобів вимагає системного підходу.

При описі таких складних систем пропонується використовувати такі принципи:

– мети;

– багаторівневого опису;

– класифікації.

Розглянемо, як можна застосувати ці принципи для систематизації та класифікації процесів ІА. Введемо такі позначення:

– $G = G\{ST, SO, NA, OK$ - мета ІА;

– множина $SS\{ST, SO\}$- структурний опис системи;

– множина $S = S\{ST, SO, NA\}$ - стани системи;

– λ - вхідний потік заявок на ІА;

– μ - потік виконання заявок системою ІА;

– $V = V\{ST, UA, CA\}$ - множина загроз;

– $A = A\{ST, UA, CA\}$ - множина атак;

– $U = U\{ST, SO, NA\}$ - множина вразливостей.

Зауважимо, що дійсно коректне розв'язання завдань ІА учасників віддаленої електронної взаємодії не є тривіальним процесом, тому під час вибору та впровадження тих чи інших рішень необхідно розуміти можливості, обмеження та рівень довіри до використовуваних механізмів і засобів автентифікації.

2.2 Класифікація процесу та систем автентифікації суб'єктів доступу

Спробуємо виокремити основні цілі створення СІА. Двома основними цілями процесу автентифікації є:

– аутентифікація сторін під час віддалених електронних відносин;

– аутентифікація джерела даних.

Аутентифікація сторін, як правило, є онлайн-сервісом безпеки, до основних завдань якого належать:

– підтвердження пред'явленого ідентифікатора з метою надання доступу до інформаційного ресурсу або мережі;

– ідентифікація власника електронного підпису (ЕП) і забезпечення безвідмовності при застосуванні ЕП;

– встановлення довірчих відносин під час віддалених електронних відносин.

Основною метою СІА є підтвердження ідентифікації зареєстрованого в ІС користувача для управління його доступом.

Опишемо типи СІА:

1) локальна. Служби автентифікації розташовані на кожному пристрої, там же відбувається процес автентифікації за допомогою одного валідатора (механізму А, якому довіряє власник ресурсу) і ухвалюється рішення про доступ. Прикладами локальної А є персональний комп'ютер, ноутбук, стільниковий телефон;

2) пряма. Власник ресурсу в процесі А довіряє одному валідатору, розташованому всередині захищеного периметра локальної обчислювальної мережі. Прямий А називається тому, що всі користувачі, які бажають отримати доступ до ресурсу, безпосередньо проходять процес А, пред'являючи аутентифікатор валідатору. Прикладом СІА прямого типу є невеликі організації чисельністю до 20 робочих місць;

3) доменна. Відрізняється від прямої тим, що одному валідатору, розташованому всередині захищеного периметра локальної обчислювальної

мережі, довіряють власники багатьох ресурсів, розташованих у ЛОМ. У кількісному відношенні СІА доменного типу переважають у сегментах малого та середнього бізнесу;

4) ієрархічна. Відрізняється від доменної наявністю підпорядкованих доменів. В ієрархічній схемі СІА доступ користувачам може надавати підлеглий домен, проте в центрі є БДНЗ користувачів і право управління доступом. Типовим прикладом таких СІА є організація, що має широку філіальну мережу;

5) розподілена мережева. Відрізняється від доменної наявністю безлічі доменів, пов'язаних між собою трастовими (довіреними) відносинами. У кожному домені незалежно здійснюється процес А і приймається рішення про доступ. Такі СІА характерні для великих корпорацій і холдингів;

6) мостова. Відрізняється від розподіленої мережевої наявністю ДТС. СІА мостового типу характерні для відомчої взаємодії з розвиненим електронним документообігом;

7) браузерна. Відрізняється від мостової механізмом А, заснованим на організації захищеного каналу зв'язку клієнт-сервер на сесійному рівні. ДТС може перебувати на цьому ж сервері. Одним із яскравих прикладів СІА браузерного типу є портал державних послуг;

8) браузерна з трансляцією довіри. Призначена для забезпечення доступу до хмарних сервісів та ІС, у яких немає облікового запису цього користувача. Відрізняється від браузерної наявністю завдання транслювання довіри до аутентифікації, яку користувач успішно пройшов у первинній ІС, в інші ІС, куди даному користувачеві необхідно надати доступ. Це завдання, як правило, розв'язують із застосуванням федеративної системи трансляції довіри.

За основними видами автентифікацію як засіб захисту від активних атак видається доцільним розділити на автентифікацію сторін (партнерів) і автентифікацію джерела даних або повідомлень.

На рисунку 2.1 показано, що у багатьох інформаційних системах процес аутентифікації асоціюють із завданнями, які можна класифікувати за їхнім цільовим призначенням:

1) для надання санкціонованого доступу. Використовується в системах управління логічним доступом до комп'ютера, корпоративної мережі, інформаційних ресурсів і сервісів. Також використовується як фільтр "свій - чужий";

2) для встановлення довірчих відносин під час віддаленого доступу. Така аутентифікація може бути взаємною (двосторонньою) і односторонньою. Типовий приклад - мережеві протоколи обміну з попереднім встановленням довірчих відносин і вироблення сеансових ключів (за допомогою симметричних криптографічних протоколів) на основі багатоходового захищеного обміну підписаною сторонами інформацією на базі PKI (протокол AH - перша частина протоколу SSL - може бути як одностороннім, так і двостороннім). Взаємодії можуть бути "суб'єкт - об'єкт" або "об'єкт - об'єкт" (наприклад, IPSec, M2M);

3) для встановлення (ідентифікації) особи власника електронного підпису, перевірки наявності повноважень на право підпису та фіксації невідворотності виконання процедури підпису електронного документа власником електронного підпису.

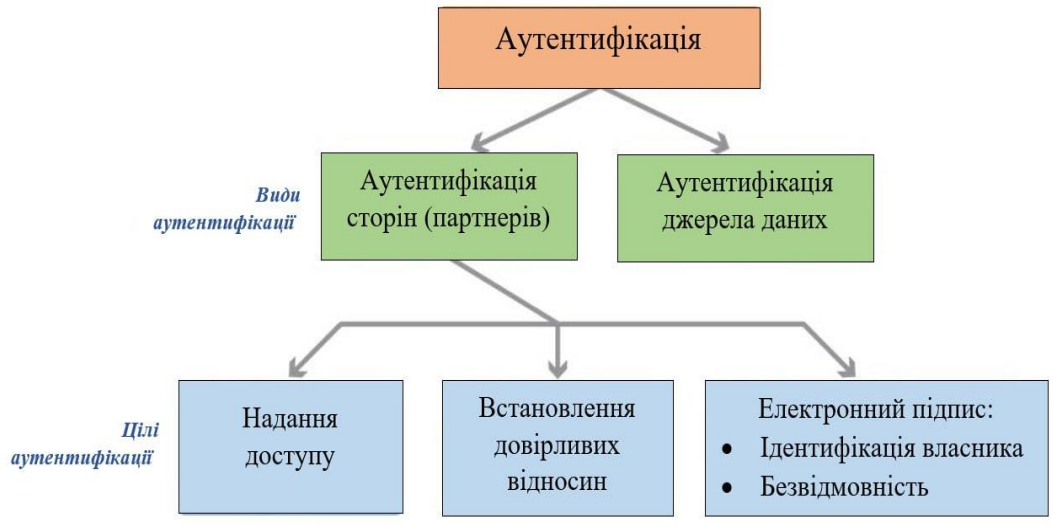

Рисунок 2.1 - Класифікація процесу аутентифікації за видами та цілями

Підсистеми автентифікації можна розрізняти за типом інформаційної системи та місцем застосування:

1) у локальній обчислювальній мережі;

2) у розподіленій корпоративній обчислювальній мережі;

3) для віддаленого доступу легальних користувачів до корпоративної мережі;

4) для доступу до хмарних сервісів з корпоративної мережі;

5) для доступу до хмарних сервісів із "недовірливого" середовища.

Крім цього, системи ідентифікації та автентифікації можна класифікувати за категоріями інформації, що зберігається й обробляється на ресурсах, до яких треба організувати доступ:

1) загальнодоступна (відкрита) інформація;

2) інформація обмеженого доступу (ДСК, персональні дані, "таємно" та ще понад 30 видів службових таємниць).

2.3 Класифікація засобів автентифікації

За рівнями довіри засоби аутентифікації можуть бути розділені на градації, розташовані в міру зростання рівня захищеності аутентифікаційної та ідентифікаційної інформації:

1) низький рівень - проста аутентифікація. Це парольна аутентифікація. Пароль не передається мережею у відкритому вигляді. Порівнюються хеші паролів;

2) середній рівень - посилена аутентифікація:

– одноразовий пароль;

– багаторазовий пароль (пароль облікового запису користувача) спільно з одноразовим паролем (OTP);

– некваліфікований сертифікат доступу.

3) високий рівень – сувора аутентифікація:

– кваліфікований сертифікат доступу, секрет (ключ підпису) зберігається в реєстрі;

– кваліфікований сертифікат доступу, секрет (ключ підпису) зберігається на незахищеному носії (дискета, флеш-пам'ять);

– кваліфікований сертифікат доступу, секрет (ключ підпису) зберігається в захищеному сховищі (після генерації встановленим на засобах обчислювальної техніки криптопровайдером криптопровайдер імпортується з оперативної пам'яті до смарт-картки, USB-ключа), доступ до секрету захищений PIN-кодом;

– кваліфікований сертифікат доступу, секрет (ключ підпису) генерується засобами смарт-картки (USB-ключа) і ніколи не залишає захищену пам'ять чипа; доступ до секрету захищений PIN-кодом;

– кваліфікований сертифікат доступу, секрет (ключ підпису) генерується засобами смарт-картки (USB-ключа) і ніколи не залишає захищеної пам'яті чипа; доступ до секрету захищений PIN-кодом, приналежність ключового носія конкретному користувачеві додатково доводять біометричними способами.

Класифікацію автентифікації за рівнями достовірності результатів найкраще вести на основі простої шкали за аналогією зі встановленими видами електронного підпису: простий, посилений і строгий. Наведемо короткий опис трьох рівнів довіри автентифікації.

Проста аутентифікація ґрунтується на традиційних багаторазових паролях і застосовується з обов'язковим узгодженням засобів використання пароля та способів його обробки (наприклад, хешування, шифрування під час передавання та зберігання). Системи простої аутентифікації на основі багаторазових паролів зазвичай мають низьку стійкість до атак, оскільки, як правило, вибір аутентифікаційної інформації ґрунтується на відносно невеликому виборі слів. Посилена аутентифікація базується на більш стійкій до атак технології OTP (One-Time-Password, одноразовий пароль), де для кожного запиту на доступ використовується новий пароль, дійсний тільки для одного входу в систему. До посиленої автентифікації може бути віднесено механізм, заснований на технології електронного підпису з використанням цифрового сертифіката доступу, випущеного ЗЦ із невизначеним рівнем довіри.

Поняття "строга автентифікація" через часте, але не завжди правильне вживання потребує більш повного розгляду. Основою ідеєю є те, що сторона, яка перевіряється, у процесі захищеного обміну інформацією, що послідовно підписується сторонами, доводить, що сторона, яка перевіряє, має попередньо розподілений у безпечний спосіб секрет (як правило, йдеться про закритий ключ).

У таблиці 2.1 представлемо можливість виконання завдань забезпечення доступності, цілісності та конфіденційності даних користувача для запропонованих рівнів довіри аутентифікації.

Таблиця 2.1 - Зв'язок типів автентифікації з безпекою користувацьких даних на стороні клієнта

Типи аутентифікації	Доступність	Цілісність	Конфіденційність
Проста (пароль)	+	–	–
Посилена (OTP)	+	–	–
Посилена (X.509, виданий УЦ з невизначеним рівнем довіри)	+	+	–
Сувора (X.509, виданий довіреним УЦ	+	+	+

2.4 Моделювання процесу аутентифікації для дослідження надійності та безпеки її результатів

На рисунку 2.2 вказано, що дослідження функціональної надійності систем ідентифікації та автентифікації включає:

– опис складу та змісту процесів і систем ідентифікації та автентифікації;

– визначення цілей аналізу та розподіл їх за рівнями моделювання;

– аналіз надійності процесів і систем ідентифікації та аутентифікації;

– оцінку результатів і вироблення рекомендацій щодо вдосконалення процесів і систем ідентифікації та автентифікації з позиції надійності.

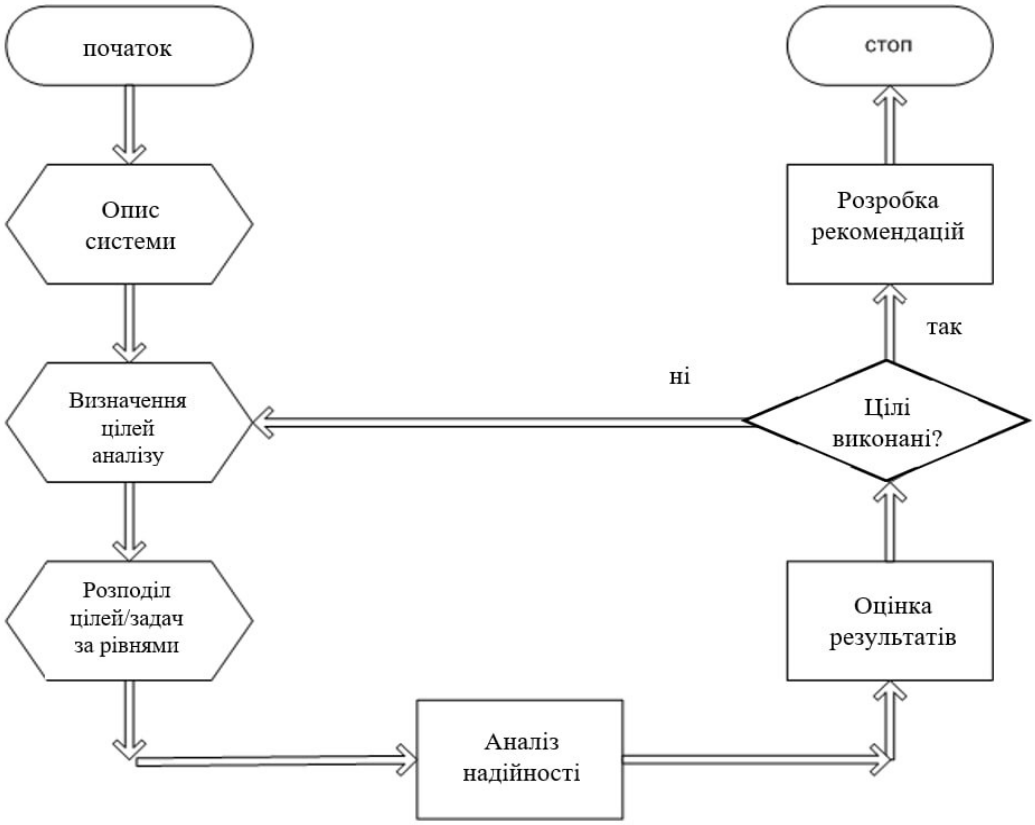

Рисунок 2.2 - Алгоритм дослідження функціональної надійності СІА

Моделювання СІА умовно можна розділити на три рівні.

Верхній (перший) рівень - моделі поведінки СІА як єдиного цілого. За такого підходу СІА є окремою системою, тобто являє собою підсистему розглянутої ІС. У цьому разі з традиційної тріади безпеки пріоритети для СІА мають бути вибудувані в такому порядку:

1) доступність СІА для всіх заявок на автентифікацію;

2) цілісність ПЗ системи;

3) конфіденційність ідентифікаційної та автентифікаційної інформації суб'єктів доступу.

Верхній (перший) рівень - моделі поведінки СІА як єдиного цілого. За такого підходу СІА є окремою системою, тобто являє собою підсистему розглянутої ІС. У цьому разі з традиційної тріади безпеки пріоритети для СІА мають бути вибудувані в такому порядку:

1) доступність СІА для всіх заявок на автентифікацію;

2) цілісність ПЗ системи;

3) конфіденційність ідентифікаційної та автентифікаційної інформації суб'єктів доступу.

Яскравим прикладом моделювання на верхньому рівні є моделі, засновані на застосуванні добре розвиненого до теперішнього часу математичного апарату систем масового обслуговування (СМО). За допомогою моделей СМО можна визначити необхідні інтегральні характеристики СІА під час їх проектування. При цьому вхідними (заданими) параметрами зазвичай є дані про вхідний потік заявок на обслуговування і самий процес. Як вихідні параметри, як правило, визначаються час обслуговування заявок і час очікування (затримки). Використовуючи модель верхнього рівня, можна виконати грубі оцінки надійності СІА.

Згідно з прийнятою в цій роботі методикою розглянемо спочатку надійність і безпеку СІА, потім послідовності процедур, що входять до неї, а за необхідності опустимося на нижчі рівні загальної моделі.

На першому (верхньому) рівні моделювання СІА розглядають як один елемент із вхідними і вихідними характеристиками, частину з яких задають, а частину визначають, як правило, добре розвиненими аналітичними методами.

Під час проектування СІА необхідно виконати попередній розрахунок її продуктивності з урахуванням обраних технологій, засобів і режиму роботи. Головною метою розрахунків є забезпечення заданих характеристик доступності інформаційних ресурсів і технологій, необхідних для виконання службових обов'язків співробітниками, при дотриманні конфіденційності та цілісності збереженої, переданої й оброблюваної інформації. Існуючі методи таких досліджень, як правило, засновані на застосуванні автоматизованого опрацювання даних. Отримувані за допомогою СМО результати зазвичай пов'язані з розрахунком імовірнісних характеристик часу опрацювання заявок у СІА за заданих характеристик вхідного потоку і процесу обслуговування заявок. Під час проектування найчастіше розв'язують обернену задачу: визначення необхідного часу опрацювання заявок згідно з висунутим замовником технічним завданням (зокрема, таким, що враховує інтенсивність потоку λ) за заданого

рівня середньої затримки часу опрацювання вимог на аутентифікацію. Іншим прикладом зворотної задачі є розрахунок обов'язковості опрацювання СІА всіх заявок на аутентифікацію від легальних користувачів ІС. У результаті розрахунків в обох випадках мають виходити величини параметрів СІА, які можуть бути змінені на етапах проектування системи.

Найчастіше, особливо на ранніх стадіях проектування, у проектувальника відсутній достатній рівень знань імовірнісної структури вхідних потоків заявок і середнього часу їх обслуговування. Тому досліднику необхідно додатково оцінювати вплив апріорних припущень про ймовірнісні характеристики вхідних потоків і потоків обслуговування. Як правило, заздалегідь виконують аналіз припущень, виходячи з умов, для яких проектують СІА.

Так, найчастіше припускають, що λ відома. Це припущення ґрунтується на тому, що зазвичай у технічному завданні на проектування вказують кількість запитів, що надходять у СІА, за певний період. При цьому невизначеність знань проектувальника про вхідний потік заявок відбивається в припущенні про дисперсію часового інтервалу між надходженнями сусідніх запитів.

Оцінка часових характеристик СІА передбачає визначення інтенсивності опрацювання заявок, що гарантує виконання заданих обмежень на середній час проходження вимог у системі:

$$\frac{1}{\mu} < \frac{1}{\lambda}, \lambda < \mu, \tag{2.1}$$

де μ - інтенсивність потоку обслуговування.

У багатьох практичних задачах потоки подій припускають такими, що володіють трьома основними властивостями: стаціонарністю, ординарністю та відсутністю післядії. Стаціонарними називаються потоки, у яких імовірність надходження певної кількості заявок протягом певного проміжку часу не залежить від початку відліку часу, а визначається тільки довжиною проміжку. Ординарність означає, що ймовірність появи двох і більше подій на досить малому інтервалі часу мала порівняно з імовірністю появи однієї події та

ймовірністю не появи жодної. Відсутність післядії означає незалежність кількості подій, що потрапили в будь-який із проміжків часу, що не перекриваються між собою, від кількості подій, що потрапили в інші проміжки.

Найпростіший потік описується формулою Пуассона

$$P_n(t) = \frac{(\lambda t)^n}{n!} e^{-\lambda t}, \qquad (2.2)$$

де n - число подій, що настали в інтервалі часу (0, t).

Для різних типів СМО з урахуванням характеру математичних моделей їхньої побудови прийнято трибуквене позначення вигляду *A*/*B*/*m*, де *A* і *B* описують розподіл часу між заявками та часом їхнього обслуговування відповідно; m - кількість каналів.

Параметри *A* і *B* приймають значення з такого набору символів: *M* - показовий розподіл, *Ea* - розподіл Ерланга порядку a, *D* - детермінований розподіл, *G* - розподіл загального вигляду. Іноді вказують довжину черги *k*, тобто *A/B/m/k*. При цьому ємність накопичувача повинна вміщати не менше *k* заявок.

Найважливішою характеристикою кожного каналу є час обслуговування заявки. Час обслуговування слід вважати випадковою величиною, повною характеристикою якої є закон розподілу

$$F(t) = P[t_{обсл} < t], \qquad (2.3)$$

де $P[t_{обсл} < t]$ - імовірність того, що час обслуговування не перевищує деякого значення *t*.

Закон розподілу *F(t)* може бути різного виду. У теоретичних роботах і практичних додатках найбільшого поширення набув показовий закон. Тип моделі, розподіл потоків заявок і їхнє опрацювання на стадіях проектування визначаються технічним завданням для конкретної СІА.

На другому рівні моделювання, виходячи з попередньої оцінки ризиків, враховується деталізація складових частин СІА з метою уточнення впливу на доступність, конфіденційність і цілісність певних параметрів Для моделювання процесу аутентифікації слід розділити його на однорідні за функціональними та ймовірнісно-статистичними характеристиками блоки. При цьому різні блоки мають істотно відмінні характеристики за часом. Наприклад, процедура реєстрації проводиться одноразово і може бути відносно короткою за часом. Зберігання ідентифікаційних даних, АІ та електронних посвідчень - тривала процедура, до якої можуть бути застосовані ймовірнісні та статистичні методи. Решта процедур (пред'явлення ідентифікаторів, ідентифікація, пред'явлення АІ, перевірка достовірності ІД за допомогою АІ, валідація, ухвалення рішення) тісно пов'язані з часом виконання процедур і багаторазово повторюються протягом життєвого циклу АІ - як правило, один раз на день. У підсумку виокремлюємо такі блоки:

1) реєстрація - не пов'язана з часом (стаціонарний процес);

2) зберігання - пов'язане з часом, тривала процедура, як правило, для суворої аутентифікації від року до трьох років;

3) пред'явлення ІД та ідентифікація - зазвичай процедура триває частки секунди, можливі помилки користувачів (часта подія) і збої сервера зберігання облікових даних користувачів (рідкісна подія);

4) пред'явлення АІ та протоколів обміну - відмови (відмови апаратного і програмного компонентів, випадкові, невипадкові помилки користувачів, атаки - такі події відбуваються дуже рідко);

5) валідація - ймовірність відмови для корпоративних закритих систем мала, для ІССК велика;

6) ухвалення рішення ("свій - чужий") - проста процедура;

7) процес ухвалення рішення (позитивний або негативний результат проходження процедури автентифікації) означає відповідь "так" або "ні" для пропуску (або відмови в проході) до наступної процедури (перевірці

відповідності облікового запису та ідентифікатора певній ролі доступу для подальшої авторизації користувача).

За процедурою зберігання секрету та ЕП слідує процедура пред'явлення ІД, АІ, ЕП для відпрацювання протоколу аутентифікації. Спосіб пред'явлення автентифікатора повністю залежить від протоколу автентифікації та його налаштувань. Наприклад, для аутентифікації клієнта SSL/TLS і серверів у протоколі IPSec цей процес відбувається в автоматичному режимі. Процедури пред'явлення секрету (підпис повідомлень у вигляді відгуку претендента) і перевірки валідності ЕП є найтривалішими (близько половини, а то й однієї секунди кожна). Процедура ухвалення рішення триває секунди і відбувається на сервері аутентифікації. Отже, можна уявити динамічні процедури (пред'явлення, протоколів, валідації та ухвалення рішення) у графічній формі у вигляді структурних блоків (рисунок 2.3).

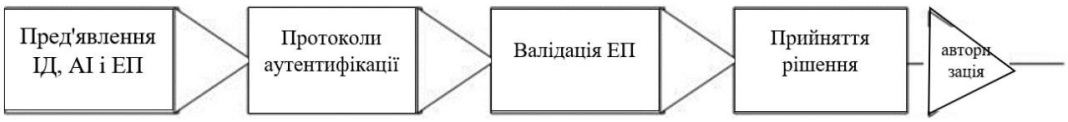

Рисунок 2.3 - Послідовність процедур аутентифікації

Для ІС з великим числом користувачів однією з проблем, що часто зустрічаються, є продуктивність СІА, що характеризується потоком μ обробки вхідних заявок λ на ІА. Для більшості ІС ця проблема не актуальна, оскільки інтенсивність вхідного потоку легко розрахувати в піковому навантаженні (початок робочого дня), і умова $\frac{\lambda}{\mu} \le 0{,}8$ може бути виконано.

Застосувавши класичну задачу подолання ешелонованого захисту інформації (оборони), можна показати, згідно рисунка 2.3, найпростіші моделі процесу автентифікації Уявімо вибрані блоки, що беруть участь у процесах ІА, у вигляді низки послідовно розташованих груп пристроїв r_i (рисунок 2.4), що обслуговують потік заявок з інтенсивністю λ і середнім часом обслуговування *t*. Заявки, які не були обслужені першим пристроєм, потрапляють на другий

пристрій, заявки, які не були обслужені другим пристроєм, потрапляють на третій і т.д.

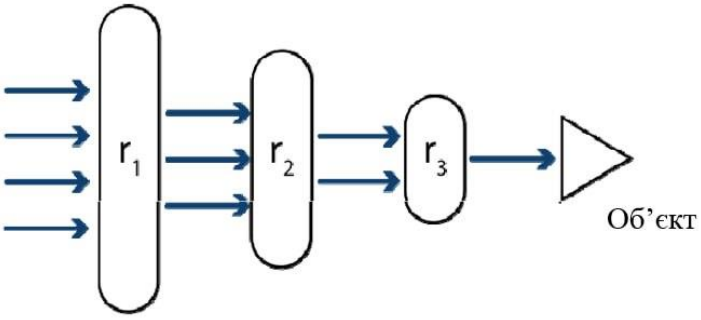

Рисунок 2.4 - Ряд пристроїв, що обслуговують потік заявок

Аналогом такої схеми являється схема подолання зловмисником ешелонованого захисту інформації. Звідси слідує, що ймовірність «прориву» зловмисника істотно зменшується від ешелону до ешелону (рисунок 2.5).

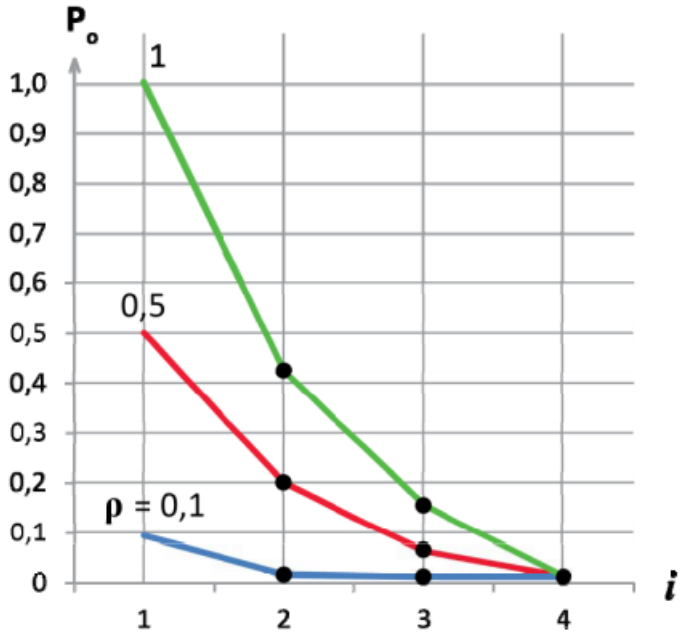

Рисунок 2.5 – Ймовірність прориву через ешелони оборони

Приклад реальних значень ймовірності відмови P_0 одноканального потоку заявок $\rho=\lambda t$ однократної парольної аутентифікації з допустимим порогом відмови P_0=0,5% представлений на рисунку 2.6.

Видно, що розрахункові значення P_0 в робочому діапазоні значень $\rho \leq 0,5$ не досягають величини 0,005 з великим запасом. Отримані співвідношення

дозволяють визначити такі параметри, як ймовірність безпомилкової роботи системи в умовах заданого потоку заявок та ймовірність безпомилкової роботи за заданий час.

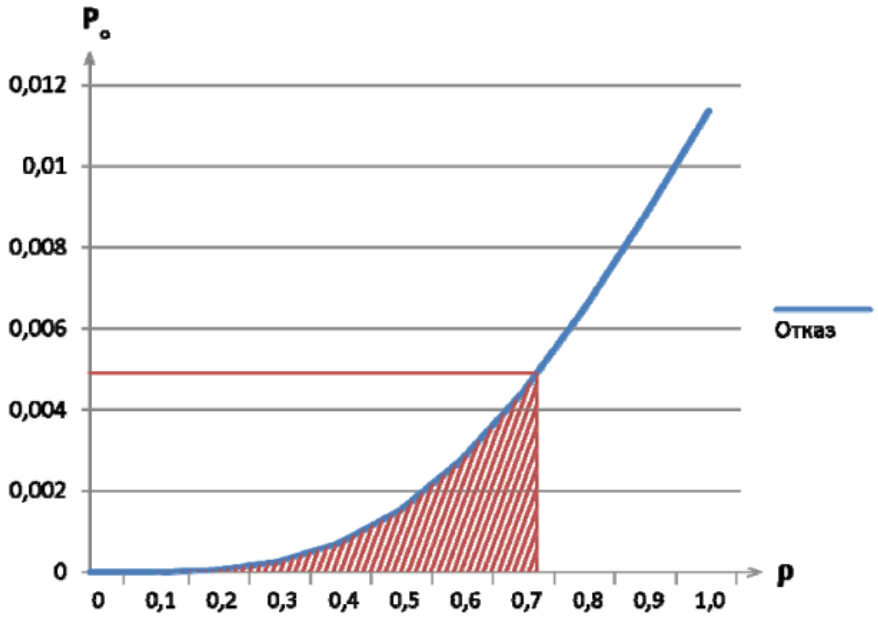

Рисунок 2.6 – Приклад допустимих значень відмов у аутентифікації

Під час подальшого розвитку моделі процедур аутентифікації її можна ускладнювати, послідовно враховуючи нові параметри. Покажемо, як можна врахувати вплив поглинання на прикладі укрупненої моделі аутентифікації. Позначимо стани системи в процесі аутентифікації:

1) реєстрацію нового користувача системи виконано;

2) здійснено підтвердження достовірності пред'явлених претендентом (користувачем) аутентифікаційних даних;

3) процедуру ухвалення рішення "свій - чужий" виконано;

4) стан відмови автентифікації легального користувача;

5) стан небезпечної відмови (автентифікація зловмисника під виглядом легального користувача).

Тепер роботу системи аутентифікації представимо у вигляді спрямованого графа станів (рисунок 2.7).

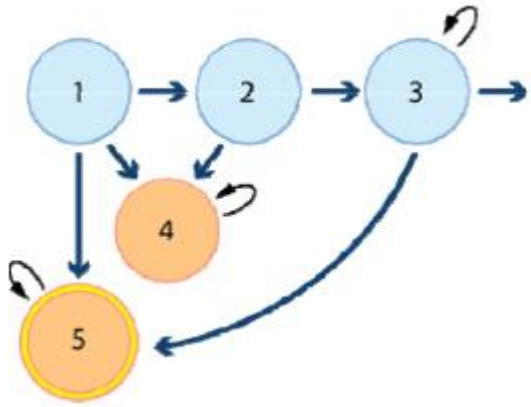

Рисунок 2.7 - Граф станів укрупненої ймовірнісної моделі аутентифікації

Імовірність переходів з одного стану в інший позначені таким чином:

- p_{12} - імовірність переходу зі стану 1 (реєстрація) у стан 2 (підтвердження автентичності пред'явлених ідентифікаторів);

- p_{14} - імовірність переходу зі стану 1 у стан 4 (відмова);

- p_{15} - імовірність переходу зі стану 1 у стан 5 (небезпечна відмова);

- p_{23} - імовірність переходу зі стану 2 у стан 3 (ухвалення рішення);

- p_{24} - імовірність переходу зі стану 2 у стан 4 (відмова);

- p_{33} - імовірність поглинання в стані 3; зауважимо, що $p_{33} \neq 1$;

- p_{35} - імовірність переходу зі стану 3 у стан небезпечної відмови;

- p_{44} - імовірність поглинання в стані відмови, при цьому $p_{44} = 1$;

- p_{55} - імовірність поглинання в стані відмови, при цьому $p_{55} = 1$.

Застосуємо до цієї запропонованої моделі теорію ланцюгів Маркова. Тоді матриця переходів для такої схеми може бути записана у такому вигляді:

	1	2	3	4	5
1	0	ρ_{12}	0	ρ_{14}	ρ_{15}
2	0	0	ρ_{23}	ρ_{24}	0
3	0	0	ρ_{33}	0	ρ_{35}
4	0	0	0	1	0
5	0	0	0	0	1

Приведемо отриману матрицю для перехідних імовірностей до канонічного вигляду, поставивши стани, що поглинають, першими:

$$P = \cdots \begin{pmatrix} I & O \\ R & Q \end{pmatrix} \cdots =$$

	4	5	1	2	3
4	1	0	0	0	0
5	0	0	0	0	0
1	ρ_{14}	ρ_{15}	0	ρ_{12}	0
2	ρ_{24}	0	0	0	ρ_{23}
3	0	ρ_{35}	0	0	ρ_{33}

Фундаментальна матриця обчислюватиметься за формулою $N = (I - Q)^{-1}$.

Матриця ймовірностей поглинання B = NR.

3 ФОРМУВАННЯ РІВНІВ ДОВІРИ ПРИ АУТЕНТИФІКАЦІЇ СУБ'ЄКТІВ ДОСТУПУ

3.1 Визначення інфраструктури довіри під час аутентифікації

У міжнародному стандарті ISO/IEC 29115 / ITU-T X.1254 "Information technology - Security techniques - Entity authentication assurance framework" наголошується, що чимало електронних транзакцій у системах на базі інформаційно-комунікаційних технологій або між такими системами повинні здійснюватися згідно з вимогами безпеки, що залежать від усвідомленого чи заданого рівня впевненості в автентичності залучених у ці процеси сутностей. Ці вимоги можуть включати захист активів або ресурсів від НСД, для чого використовується механізм контролю доступу, та/або забезпечення підзвітності на основі ведення журналів реєстрації відповідних подій.

У міжнародному стандарті міститься керівництво з приведення інших інфраструктур довіри до певних чотирьох рівнів і керівництво з обміну результатами транзакцій, використовуваними для аутентифікації. Насамкінець наводиться докладний посібник із захисту АІ, що дає змогу перевірити автентичність ідентифікаційної інформації (ІІ).

У документі представлено інфраструктуру довіри, що включає:

- чотири рівні довіри щодо аутентифікації сутності;
- керівництво з відображення інших схем довіри щодо автентифікації на чотири LoA;
- посібник з обміну результатами автентифікації, що ґрунтуються на чотирьох LoA;
- настанову щодо методів контролю, які повинні використовуватися з метою зниження небезпеки загроз для аутентифікації.

Кожен LoA описує ступінь упевненості в процесах, що призводять до автентифікації, включно із самим процесом автентифікації, забезпечуючи довіру щодо того, що сутність, яка використовує конкретну ІІ, є тією самою, для якої ця

ідентифікаційна інформація була призначена. Сутність може бути як людиною, так і об'єктом, що не є фізичною особою.

LoA1 являє собою найнижчий рівень довіри, а LoA4 – найвищий (таблиця 3.1). Яким має бути LoA в кожній конкретній ситуації залежить від безлічі факторів. Здебільшого визначення необхідного LoA ґрунтується на ризику: наслідки помилки автентифікації та/або неналежного використання реєстраційних даних, заподіяна внаслідок цього шкода, а також імовірність їх виникнення. Вищі LoA повинні використовуватися для більш високого передбачуваного ризику.

Таблиця 3.1 - Рівні довіри відповідно до міжнародного стандарту ISO/IEC 29115 / ITU-T X.1254

Рівень	Опис
1 – низький	Незначна впевненість або відсутність впевненості в заявленій автентичності
2 – середній	Суттєва впевненість у заявленій автентичності
3 – високий	Висока впевненість у заявленій автентичності
4 – дуже високий	Дуже висока впевненість у заявленій автентичності

Інфраструктура довіри визначає вимоги та керівництва щодо реалізації кожного з чотирьох LoA.

На LoA1 має місце мінімальна впевненість у заявленій достовірності сутності, але після кількох послідовних подій автентифікації виникає певна впевненість у тому, що сутність справжня. Цей LoA використовують, коли помилкова аутентифікація пов'язана з мінімальним ризиком.

Особливі вимоги до механізмів автентифікації відсутні, вони мають забезпечувати лише якусь мінімальну довіру. Цей рівень не вимагає застосування криптографічних методів.

На LoA2 має місце значна впевненість у заявленій автентичності сутності. Він використовується, коли помилкова аутентифікація пов'язана з помірним

ризиком. На цьому рівні прийнятна однофакторна аутентифікація. Мають використовуватися засоби контролю, що дають змогу знизити ефективність атак перехоплення інформації та підбору пароля в режимі реального часу. Необхідні також засоби контролю для захисту від атак, спрямованих на облікові дані, що зберігаються.

На LoA3 має місце висока впевненість у заявленій автентичності сутності. Він використовується, коли помилкова аутентифікація пов'язана зі значним ризиком. На цьому рівні потрібна багатофакторна аутентифікація. Будь-яка секретна інформація, обмін якою здійснюється в рамках протоколів аутентифікації, має бути криптографічно захищена як під час передання, так і в черговому режимі (при цьому LoA3 не вимагає застосування запитно-відповідного криптографічного протоколу). На LoA3 будь-які вимоги до створення або зберігання облікових даних не передбачаються; ці дані можуть зберігатися або створюватися в комп'ютерах загального призначення або за допомогою спеціалізованого апаратного обладнання.

LoA4 характеризується дуже високою впевненістю в заявленій справжності сутності. Він використовується, коли помилкова аутентифікація пов'язана з дуже високим ризиком. На цьому рівні забезпечується найвищий рівень впевненості щодо аутентифікації. LoA4 схожий на LoA3, але на ньому додаються вимоги до особистого підтвердження автентичності для сутностей, які є людьми, і застосування захищених від проникнення пристроїв для зберігання всіх секретних криптографічних ключів. Крім того, персональні дані та інші відомості конфіденційного характеру, включені в протоколи автентифікації, мають бути криптографічно захищені як під час передачі, так і в черговому режимі.

Вибір належного LoA слід здійснювати на основі оцінювання ризику транзакцій або сервісів, у межах яких сутності проходитимуть автентифікацію. Міжнародний стандарт ISO/IEC 29115 містить приклад матриці оцінки потенційних наслідків помилкової аутентифікації для різних LoA. Загрози на етапі автентифікації охоплюють загальні загрози та загрози, пов'язані з

використанням облікових даних у межах автентифікації. До загальних загроз автентифікації належать: використання шкідливого ПЗ (наприклад, віруси, троянські програми, клавіатурні шпигуни), соціальна інженерія (наприклад, підглядання, крадіжка апаратних пристроїв і PIN-кодів), помилки користувачів (наприклад, ненадійні паролі, невикористання заходів захисту автентифікаційної інформації), помилкова відмова, несанкціоноване перехоплення та/або зміна даних автентифікації під час передавання, відмова в обслуговуванні, не справжність процедур. За винятком випадку використання багатофакторної автентифікації, засоби контролю загальних загроз автентифікації не входять до сфери дії міжнародного стандарту ISO/IEC 29115.

Існує велика кількість загроз щодо облікових даних, що містять ПДн, під час їх використання для цілей аутентифікації. У документі перелічено деякі поширені категорії загроз, що мають місце під час використання облікових даних, і наводяться конкретні приклади реалізації цих загроз. Крім того, міжнародний стандарт ISO/IEC 29115 містить перелік заходів захисту від зазначених категорій загроз.

Аналіз міжнародних і національних стандартів, що регламентують процеси ІА, показав:

– у рамках діяльності Міжнародної організації зі стандартизації (International Organization for Standardization), Міжнародної електротехнічної комісії (International Electrotechnical Commission) і Міжнародного союзу електрозв'язку (International Telecommunication Union) розроблено систему міжнародних стандартів, що регламентують різні аспекти ІА;

– стандарти, що входять до складу системи міжнародних стандартів, постійно вдосконалюються, а основні положення систематично переглядаються відповідно до наявних можливостей їх технічної реалізації;

– як базові характеристики процесу ІА видається доцільним визначити:

1) види ідентифікації (первинна, вторинна);

2) фактори автентифікації та їх використання в процесі автентифікації (однофакторна, двофакторна, багатофакторна автентифікація);

3) форми обміну АІ (одностороння, взаємна аутентифікація);

4) види аутентифікації (проста, посилена, сувора аутентифікація).

Подальший аналіз здійснено з урахуванням базових характеристик процесу ІА. Аналіз нормативно-правових актів (НПА) щодо ЗІ від НСД в частині ІА виконувався за такими напрямами:

– наявність у НПА норм, що визначають процеси ІА суб'єктів доступу;

– наявність у правових нормах характеристик технічної реалізації процесів ІА суб'єктів доступу (у частині механізмів, засобів і видів).

Проведений аналіз включав:

– формування переліку НПА із ЗІ від НСД, у яких регламентується реалізація процесів ІА;

– визначення певних критеріїв, відповідно до яких проводиться аналіз НПА;

– аналіз НПА, що регламентують процеси ІА суб'єктів доступу відповідно до встановлених критеріїв;

– узагальнення результатів проведеного аналізу.

У рамках аналізу розглянуто 123 нормативно-правові акти, що регламентують питання ЗІ. Як основні критерії аналізу визначено:

– наявність і документальне підтвердження правових норм, відповідно до яких реалізуються процеси ІА суб'єктів доступу в ІС;

– наявність і документальне підтвердження в правових нормах характеристик технічної реалізації в частині видів, механізмів і засобів ІА суб'єктів доступу;

– способи, а також склад механізмів і засобів ІА суб'єктів доступу, які мають бути реалізовані в ІС;

– види автентифікації, необхідні для реалізації в інформаційній системі. Якщо види автентифікації не визначено конкретно, то вони можуть формуватися за наведеними правилами у таблиці 3.2.

Таблиця 3.2 - Правила визначення виду аутентифікації

Фактори автентифікації	Обмін аутентифікаційною інформацією	Вид аутентифікації
Однофакторна	Односторонній	Проста
Багатофакторна	Односторонній або взаємний	Посилена
Багатофакторна	Взаємний	Сувора

Аналіз нормативно-правових актів на предмет наявності правових норм, що регламентують процеси ІА суб'єктів доступу, показав:

– у переважній більшості НПА щодо захисту інформації від НСД процедури ІА не визначаються як обов'язкові;

– деяка кількість НПА щодо ЗІ від НСД містить правові норми, що встановлюють необхідність реалізації процедур ІА, але при цьому характеристики технічної реалізації в частині видів, механізмів і засобів ІА суб'єктів доступу не розглядаються;

– невелика частина НПА щодо ЗІ від НСД містить правові норми, що визначають необхідність реалізації процедур ІА і при цьому регламентують їхню технічну реалізацію в частині видів, механізмів і засобів ІА суб'єктів доступу;

– у НПА, що містять правові норми, як характеристики технічної реалізації визначено просту (однофакторна, одностороння) і сувору (двофакторна, взаємна) автентифікацію.

3.2 Основні характеристики процесу аутентифікації суб'єктів доступу

У процесах аутентифікації беруть участь практично всі користувачі комп'ютерів, ІС і прикладних програм. Взаємодія суб'єкта доступу із системою ідентифікації та аутентифікації починається з увімкнення комп'ютера. Після успішного проходження процедури ідентифікації, критерієм якого є збіг введеного суб'єктом ідентифікатора з наявним у системі, автентифікацію

проходять, щоб отримати доступ до комп'ютера, локальної мережі, Інтернету, розподіленої мережі, до систем захисту від НСД, до віртуальних приватних мереж. Особливе місце посідає автентифікація під час бездротового віддаленого мережевого доступу до корпоративних мереж і ресурсів, у тому числі під час переходу до хмарних обчислень.

Прикладами взаємодіючих сторін під час ідентифікації та автентифікації, крім користувачів, можуть бути процеси, відкриті ІС, логічні об'єкти тощо. Класичну задачу ІА розв'язують для взаємодії користувач - сервер ІА з поширенням цього рішення на інші об'єкти взаємодії.

У спрощеному вигляді класична процедура ІА з боку користувача (клієнтська частина) достатня для розгляду процесу ІА в закритій (локальній) корпоративній системі, де багато процедур (наприклад, процедура реєстрації користувачів) суворо регулюються внутрішніми регламентами (рисунок 3.1). З урахуванням розвитку інформаційних технологій, зокрема технологій надання доступу, і появи ІССК під час вивчення процесів ІА необхідно розглядати весь цикл процедур, що становлять процес аутентифікації.

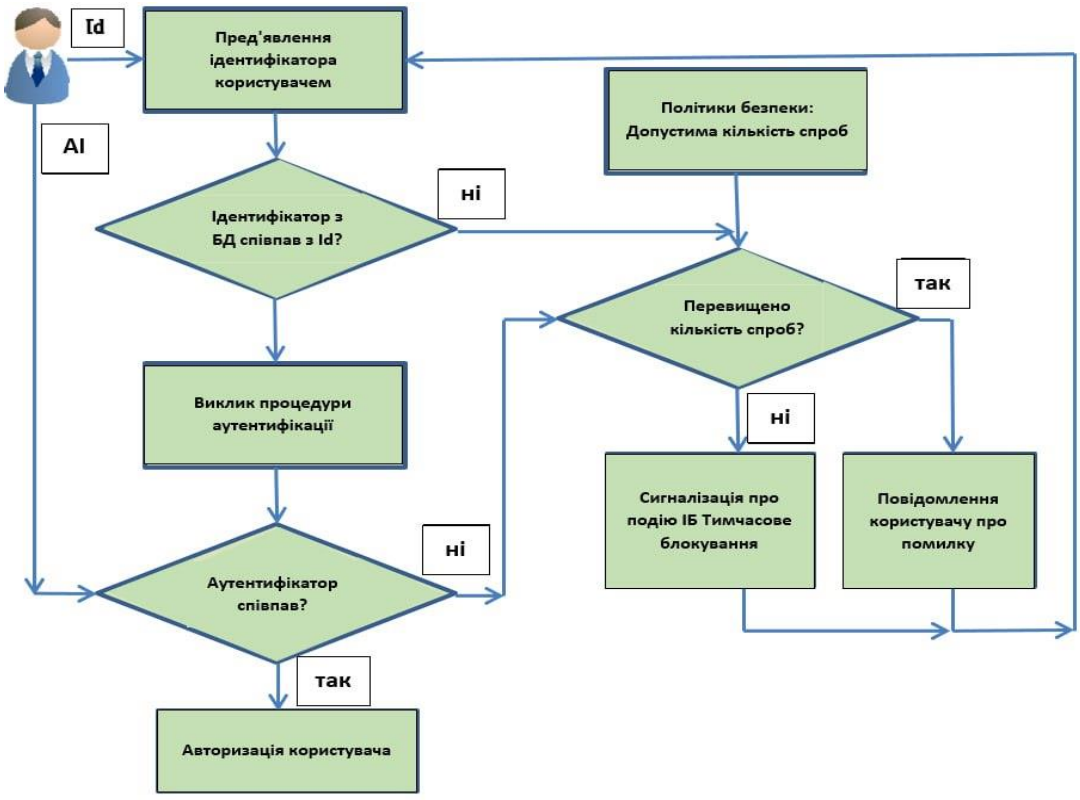

Рисунок 3.1 - Спрощена схема процесу "Ідентифікація та аутентифікація"

Перш ніж розглядати процес ІА, визначимо учасників процесу автентифікації:

– суб'єкт доступу (званий також до автентифікації аплікантом, претендентом);

– центр реєстрації, основним завданням якого є встановлення та фіксація (закріплення) зв'язку суб'єкта та його унікальної секретної ознаки - аутентифікатора. Таким центром може виступати, наприклад, віддалений центр реєстрації (ЦР) засвідчувального центру (ЗЦ), пов'язаний довірчими відносинами з даним ЗЦ;

– довірлива сторона - власник ресурсу, до якого суб'єкт претендує отримати доступ. Він перевіряє за протоколом автентифікації факт володіння суб'єктом доступу відповідним автентифікатором - секретом, який видано суб'єкту ЦР;

– сторона, що перевіряє (центр валідації, ЦВ), яка входить до складу інфраструктури відкритих ключів і виконує перевірку наявності фіксованого ЦР зв'язку "суб'єкт доступу - аутентифікатор", а також, чи є електронне посвідчення (ЕП) дійсним (валідним) на момент перевірки.

Може мати місце об'єднання окремих сутностей в одній особі, наприклад ЦР, ЦВ і сторона, що довіряє.

Ідентифікація та автентифікація включають три основні етапи. Перший етап є реєстрацією, яка розпадається на ланцюжки послідовно виконуваних взаємопов'язаних дій:

1) суб'єкт (претендент, або аплікант) звертається до ЦР з метою стати користувачем ІС. Заявник пред'являє в ЦР свої Credentials (ЕП або паперові чинні посвідчення особи, які містять присвоєні йому ідентифікаційні атрибути та їх значення). Прикладами значень ідентифікаційного атрибута є номер паспорта, номер посвідчення, СНІОР, ІНПП);

2) ЦР перевіряє пред'явлені паперові документи на автентичність і дійсність (валідація). Пред'явлене електронне посвідчення також перевіряється

на предмет достовірності змісту та його дійсності (валідація). Перевіряють унікальність сукупності пред'явлених ідентифікаційних атрибутів, проводять їхню верифікацію (перевірку за допомогою запитів, як правило, у державні реєстри) і визначають ступінь зв'язку ідентифікаційних даних з особою заявника. Якщо хоч одна з перерахованих умов (унікальність, підтвердження з офіційних джерел, ступінь прив'язки цифрових даних до суб'єкта) не відповідає вимогам і рівням доведення до отриманих результатів, прийнятим в ІС, то аплікант отримує відмову в реєстрації;

3) на підставі виконаної перевірки ЦР створює обліковий запис для суб'єкта у своїй базі даних для доступу до інформаційних ресурсів (ресурсу), що містить унікальний ідентифікатор, присвоєний новому суб'єкту доступу, і всю перевірочну інформацію, пов'язану з цим суб'єктом;

4) на основі отриманого облікового запису ЦР видає/реєструє секрет (аутентифікатор), асоційований із суб'єктом. Найсуворішим секретом є секретний ключ, який згідно з нормативно-правовою базою може бути сформований або самим суб'єктом, або ЦР. Для кожного секретного ключа на основі відповідного відкритого ключа в ЦР формується сертифікат ключа підпису (електронне засвідчення, у західних документах аналогом є Credentials - частина облікового запису), що пов'язує секретний ключ (аутентифікатор) з його власником;

5) останньою процедурою реєстрації є видача виданих ЦР автентифікатора та ЕУ суб'єкту.

Другий етап аутентифікації - це обмін аутентифікаційною інформацією з метою підтвердження автентичності пред'явленого ідентифікатора. У його рамках виконуються такі дії:

1) зберігання секрету (аутентифікатора) та ЕП. Найкращим засобом зберігання секретного ключа (ключа перевірки підпису) є застосування для генерації, зберігання та використання пристроїв класу SSCD (Secure Signature Creation Device - пристрій безпечної генерації підпису). Якщо у вигляді аутентифікатора використовується інший секрет (пароль, одноразовий пароль

тощо), то залежно від типу організації, де працює користувач, управління секретом підпорядковується певним політикам безпеки. Наприклад, у низці державних органів для автентифікації в деяких додатках строго через певний період генеруються N-символьні паролі за законом випадкових чисел і відразу автоматично записуються в захищену пам'ять електронних ключів таким чином, що користувач навіть не знає свого пароля;

2) ініціювання обміну шляхом пред'явлення претендентом ідентифікатора довіряючій стороні. Найпростішим прикладом пред'явлення ідентифікатора є введення логіна після увімкнення комп'ютера або під час входу в електронну пошту (у цьому прикладі логін збігається з назвою персональної поштової скриньки). Після введення претендентом логіна система ідентифікації та аутентифікації (СІА) порівнює пред'явлений ідентифікатор із зареєстрованим у базі користувачів і в разі збігу просить пред'явити аутентифікатор для підтвердження автентичності ідентифікатора;

3) процедура обміну аутентифікаційною інформацією. Найпростішим автентифікатором є пароль. У сучасних протоколах мережевої автентифікації зазвичай багаторазовий пароль не передається мережею у відкритому вигляді. Одноразові паролі передаються мережею у відкритому вигляді, однак для їхньої генерації використовується вектор початкової ініціалізації.

Третій етап називається валідацією. Перевірка валідності ЕП (сертифіката ключа підпису) - це дії, які виконуються над сертифікатом ключа підпису, що перевіряється, для того, щоб переконатися в можливості його використання.

3.3 Моделювання процедури аутентифікації

На цьому рівні проводиться моделювання процедур, що складають процес ідентифікації та аутентифікації. Покажемо, як можна моделювати окремі процедури аутентифікації.

Розглянемо процедуру реєстрації, яка є найбільш критичною для використання зловмисником. Ускладнимо модель, розглянуту в другому розділі.

Спочатку сформулюємо критерій відмови та небезпечної відмови. Для процедури реєстрації відмовою вважатимемо відсутність реєстрації для легального користувача, а небезпечною відмовою - реєстрацію зловмисника під ім'ям легального користувача.

У вигляді критеріїв функціональних відмов для розглянутої системи можна прийняти помилки в її роботі, що не призводять до зупинки виконання основних заданих функцій. Інакше кажучи, помилки і збої не повинні перевищувати певного порога, починаючи з якого система віддаленої аутентифікації може перестати виконувати заданий набір функцій.

Сума ймовірностей виходів із кожного стану є повною групою несумісних подій:

$$\sum_{i=1}^{n} P_i = 1, \tag{3.1}$$

де n - число станів системи.

Для моделювання процедуру реєстрації нового користувача в інформаційній системі спрощено можна представити у вигляді таких станів:

1) претендент на реєстрацію надіслав запит на сервер ЦР з метою зареєструватися в ІС;

2) ідентифікатори претендента надійшли на сервер разом із запитом на реєстрацію. Із сервера ЦР висилається запит на підтвердження наявності та збігу отриманих від претендента ідентифікаторів у базах, що містять ідентифікаційні дані громадян;

3) отримано відповіді на запит сервера. Якщо дані збіглися, ЦР створює обліковий запис претендента, який став новим легальним користувачем ІС;

4) ЦР створив або зареєстрував аутентифікатор нового легального користувача відповідно до його облікового запису;

5) ЦР видав користувачеві електронне посвідчення (наприклад, у вигляді сертифіката ключа перевірки підпису) та автентифікатор у разі, коли автентифікатор був створений ЦР.

У наведених позначеннях станів системи процес реєстрації можна представити у вигляді графа (рисунок 3.2).

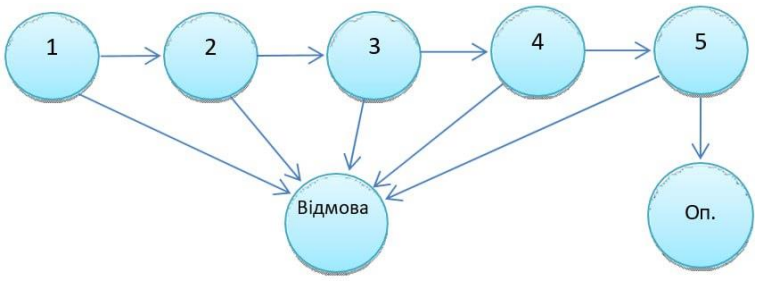

Рисунок 3.2 - Граф станів процедури реєстрації

3.4 Принципи формування рівнів довіри до методів аутентифікації

Традиційним і широко застосовуваним на заході є так званий технологічний підхід до формування рівнів довіри до результатів автентифікації. При цьому рівні довіри до автентифікації AAL (Authentication assurance levels) вводять апріорно залежно від застосовуваного методу автентифікації та попередньо оціненого власником ІС рівня ризиків. В основі цього підходу лежить упевненість у тому, що застосовані протягом багатьох років і добре досліджені методи аутентифікації дадуть очікувані результати за умови їх акуратної реалізації. Класифікація методів автентифікації (на заході - автентифікаторів) надає шкалу довіри, якою користуються багато країн під час проектування систем автентифікації. Перевагою такого підходу є простота і наочність формування рівнів довіри - вибір методу аутентифікації відразу дає уявлення про рівень довіри до результатів аутентифікації.

Його найсуттєвіший недолік - неповна прозорість визначення меж рівнів довіри не до методу, а саме до результатів аутентифікації. Це особливо актуально для найбільш "довірених" способів автентифікації, званих суворою автентифікацією, що є багатофакторною взаємною автентифікацією з організацією двостороннього, між суб'єктом доступу та об'єктом доступу, або багатостороннього (у разі використання третьої довіреної сторони) обміну

автентифікаційною інформацією . У процесі суворої аутентифікації мають використовуватися "сильні" криптографічні протоколи.

Залежно від способу генерації та зберігання автентифікаційної інформації (для суворої автентифікації це закритий ключ) рівні довіри до результатів автентифікації можна поділити на підрівні. Основним критерієм такого підрозділу є спосіб генерації закритого ключа. Якщо ключ генерується в оперативній пам'яті комп'ютера з подальшим імпортуванням у ключовий носій, рівень довіри до результатів має бути істотно нижчим, ніж у разі застосування ключових носіїв, здатних генерувати ключовий матеріал усередині спеціально спроєктованого чипа з умовою його гарантованої невидобувності.

Аутентифікатори. Під автентифікатором далі розумітимемо сукупність характеристик автентифікації: використовуваного чинника (чинників) автентифікації, способу обміну автентифікаційною інформацією (односторонній, взаємний), способу генерації, зберігання та пред'явлення автентифікаційної інформації довіряючій стороні, що довіряє, або стороні, що перевіряє (за її наявності), а також застосування криптографії. Нагадаємо, що фактором аутентифікації називають форму (вид) подання інформації. Стандарти виділяють лише три фактори.

Фактор знання: суб'єкт доступу повинен знати певну інформацію. Під час автентифікації із застосуванням фактора знання може використовуватися як автентифікаційна інформація, безпосередньо відома користувачеві, наприклад, пароль, графічний пароль, зображення, так і інформація, що дає змогу отримати доступ до автентифікаційної інформації, наприклад, одноразовий пароль або PIN-код.

Фактор володіння: суб'єкт доступу повинен володіти певним предметом, що містить аутентифікаційну інформацію. Під час автентифікації із застосуванням фактора володіння може використовуватися, наприклад, пристрій автентифікації або механізм, пристосування, що містять автентифікаційну інформацію.

Біометричний фактор: суб'єкту доступу має бути притаманна певна ознака (характеристика), інформація (дані) про яку використовується під час автентифікації.

Розглянемо автентифікатори відповідно до нормативно-правової бази та вітчизняної практики побудови СІА в роботі:

1) аутентифікатор із секретом, що запам'ятовується, який зазвичай називають паролем або, якщо це числове значення, PIN-кодом, є секретним значенням для вибору і запам'ятовування користувачем. Секрети, що запам'ятовуються, мають бути досить складними і прихованими, щоб порушник не міг відгадати або іншим чином розкрити правильне секретне значення. Секрет, що запам'ятовується, - це фактор знання. Рекомендована довжина секрету, що запам'ятовується, має бути не менше ніж 8 символів, якщо їх вибирає користувач. Секрети, що запам'ятовуються, обрані випадковим чином реєстратором, мають бути завдовжки щонайменше 6 символів і можуть бути повністю числовими. Якщо реєстратор заносить обраний секрет, що запам'ятовується, на основі його зовнішнього вигляду до чорного списку скомпрометованих значень, користувач повинен вибрати інший секрет, що запам'ятовується;

2) аутентифікатор з пошуковими секретами (одноразовими паролями) являє собою фізичний або електронний запис, де зберігається сукупність секретів, що спільно використовуються заявником і реєстратором. Заявник використовує аутентифікатор для пошуку відповідного секрету, необхідного для відповіді на запит сторони, що перевіряє. Прикладами пошукових секретів є блокнот шифрувальника, скретч-карта. Пошуковий секрет - це фактор володіння;

3) позасмуговий аутентифікатор - це фізичний пристрій, який є унікальним за адресою і може безпечно взаємодіяти зі стороною, яка перевіряє, окремим каналом зв'язку, який називається другим (додатковим) каналом. Заявник володіє і здійснює контроль над пристроєм, який підтримує приватний зв'язок цим додатковим каналом, відокремленим від основного каналу для електронної автентифікації. Найчастіше як другий канал використовують

смартфон. Повинна жорстко обмежуватися тривалість аутентифікації з використанням другого каналу. Позасмуговий аутентифікатор - це фактор володіння;

4) однофакторний OTP-пристрій генерує паролі, що динамічно змінюються (OTP - One Time Password). Ця категорія включає відокремлені від комп'ютера апаратні пристрої та програмні генератори паролів, що динамічно змінюються, встановлені, наприклад, на смартфоні. Такі пристрої мають вбудований секрет, який використовується як джерело для генерації паролів, що динамічно змінюються, і не потребує активації через другий фактор. Однофакторні OTP-пристрої аналогічні аутентифікаторам із пошуковим секретом, за винятком того, що секрети криптографічним і незалежним способом генерують аутентифікатор і довірлива сторона, а довірливу сторону порівнюють довірливою стороною. Секрет обчислюється на основі одноразового коду, який може бути сформований за поточним часом або за подією (наприклад, натисненням кнопки на пристрої OTP) або виходячи з лічильника на автентифікаторі та в сторони, що довіряє;

5) багатофакторний OTP-пристрій генерує паролі, що динамічно змінюються, для використання під час автентифікації після активації за допомогою додаткового фактора автентифікації. Сюди включаються апаратні пристрої та програмні OTP-генератори, встановлені на таких пристроях, як мобільні телефони. Другий фактор автентифікації може реалізовуватися за допомогою інтегральної клавіатури, інтегрованого біометричного зчитувального пристрою (наприклад, відбитки пальців) або прямого комп'ютерного інтерфейсу (наприклад, USB-порт). Пароль, що динамічно змінюється, відображається на пристрої і вводиться вручну для передачі довіряючій стороні. Багатофакторний OTP-пристрій - це фактор володіння, який активується за допомогою використання фактора знання або біометрії;

6) однофакторний криптографічний програмний аутентифікатор являє собою криптографічний ключ, що зберігається на диску або в незахищеній паролем флешці. Аутентифікація здійснюється шляхом підтвердження

володіння і контролю над ключем. Вихідні дані аутентифікатора сильно залежать від конкретного криптографічного протоколу, але зазвичай це якийсь вид підписаного повідомлення. Однофакторний програмний криптографічний аутентифікатор - це фактор володіння;

7) однофакторний криптографічний пристрій є апаратним пристроєм, який здійснює криптографічні операції з використанням захищеного(-их) криптографічного(-их) ключа(-ів) та надає вихідні дані аутентифікатора через пряме з'єднання з кінцевою користувацькою точкою. Пристрій використовує вбудовані симетричні або асиметричні криптографічні ключі та не потребує активації через другий фактор аутентифікації. Аутентифікація здійснюється шляхом підтвердження володіння пристроєм за допомогою протоколу аутентифікації. Вихідні дані аутентифікатора передаються шляхом прямого з'єднання з кінцевою користувацькою точкою і сильно залежать від конкретного криптографічного пристрою і протоколу, але зазвичай це якийсь вид підписаного повідомлення. Однофакторний криптографічний пристрій - це фактор володіння;

8) багатофакторне криптографічне програмне забезпечення - СВТ з криптографічним ПЗ і другий фактор у вигляді ключа з доступом до нього за паролем. Багатофакторний програмний криптографічний автентифікатор є криптографічним ключем, що зберігається на диску або будь-якому іншому "гнучкому" носії, який вимагає активації за допомогою другого фактора автентифікації. Автентифікація здійснюється шляхом підтвердження володіння і контролю над ключем. Вихідні дані аутентифікатора сильно залежать від конкретного криптографічного протоколу, зазвичай це якийсь вид підписаного повідомлення. Багатофакторний програмний криптографічний аутентифікатор - це фактор володіння, який активується за допомогою використання фактора знання або біометрії;

9) багатофакторне криптографічне апаратне забезпечення - ОЗТ із криптографічним ПЗ і окремий від ОЗТ пристрій із криптографічним ПЗ, що генерує ключі, які не можна витягти (SSCD), плюс доступ до ключа за паролем і/або біометрією. Засіб обчислювальної техніки має містити повний або частину

ЗКЗІ, пов'язану з багатофакторним апаратним криптографічним пристроєм, здатним самостійно здійснювати криптографічні перетворення для генерування одного або декількох захищених криптографічних ключових пар. Таким ЗКЗІ дозволено використовувати закритий ключ до 3 років. Для застосування закритого ключа, який ніколи не залишає захищеного розділу чипа, потрібна активація за допомогою другого фактора аутентифікації (частіше пароль або PIN-код). Іноді додатково до цього застосовується біометрія. Аутентифікація здійснюється при підтвердженні володіння пристроєм і контролю над ключем. Багатофакторний криптографічний пристрій - це фактор володіння, для застосування закритого ключа, що не витягується, використовується фактор знання та/або біометрії.

3.5 Формування та оцінювання рівнів довіри до результатів аутентифікації

Завдання формування рівнів довіри до результатів автентифікації, незважаючи на гадану складність і наявність у більшості протоколів автентифікації криптографічних алгоритмів, набагато простіше, ніж аналогічне завдання для ідентифікації, оскільки ступінь невизначеності однозначного визначення суб'єкта доступу істотно звужується під час реєстрації. У завданні автентифікації ми маємо справу із зареєстрованим користувачем системи, який успішно пройшов процедуру первинної ідентифікації за правилами конкретної ІС. Як уже згадувалося у вступі та першому розділі, мета автентифікації в кожній ІС - визначення, чи є суб'єкт, який прагне отримати доступ, тим зареєстрованим користувачем, за кого себе видає. При цьому ключовим словом є "зареєстрованим", тобто після реєстрації система аутентифікації оперує тільки з тими даними, які залишилися в ній після реєстрації нового користувача. Отже, формально довіра до процесу автентифікації та його практичної реалізації не залежить від якості проведення реєстрації, але на кінцевий результат роботи СІА якість реєстрації, і особливо ПІ, справляє вельми істотний вплив. Зауважимо, що відповідь на запитання про зв'язок особистості користувача з його унікальним

ідентифікатором (у найпростішому випадку з логіном) і зареєстрованою АІ (у найпростішому випадку з паролем) визначається виконанням вимог конкретної ІС до реєстрації нового користувача. Наприклад, якщо для реєстрації достатньо пред'явити копію паспорта, то довіра до цього зв'язку буде практично нульова, оскільки до копії за допомогою сучасних засобів техніки легко можуть бути внесені зміни, наприклад, замінено фотографію. можна зробити висновок, що складовими довіри до результатів автентифікації є функціональна надійність і безпека роботи СІА, достовірність результатів ІА і безпека АІ та ідентифікаційних даних. При цьому основним інструментом аналізу слугує оцінка ризиків. Перша ІНП пов'язана з необхідністю захисту АІ від несанкціонованого доступу протягом усього життєвого циклу. Друге - з відповідним (адекватним) вибором методу автентифікації, що визначається поєднанням чинників автентифікації, способів обміну АІ та застосовуваного протоколу обміну "претендент - сервер автентифікації".

3.6 Критерії довіри до результатів автентифікації

Результати автентифікації складається з таких компонентів:

- довіри до надійності результатів ПІ під час реєстрації нового користувача (що характеризує якість ПІ) - наскільки привласнений унікальний у даній інформаційній системі ідентифікатор і співвіднесені з ним ідентифікаційні дані відповідають суб'єкту, тобто наскільки достовірно визначено, що заявник є тим суб'єктом, за кого себе видає;

- довіри до забезпечення конфіденційності секрету (інформації, що аутентифікує) протягом усього його життєвого циклу. Приклади: пароль у разі простої аутентифікації або закритий ключ доступу в разі суворої аутентифікації - умови його генерації, зберігання, використання, утилізації;

- довіри до коректності реалізації методів автентифікації, що включають організацію обміну автентифікаційною інформацією між заявником і сервером автентифікації (односторонній або взаємний обмін), фактори автентифікації, що

використовуються при цьому, і протоколи обміну. Фактори аутентифікації схильні до атак.

Планований до використання протокол має відповідати заданому рівню довіри до методу аутентифікації.

Спосіб оцінювання довіри до результатів аутентифікації. На підставі сформульованих критеріїв запропоновано спосіб оцінювання довіри до результатів автентифікації суб'єкта доступу в просторі безрозмірних параметрів, у котрому узагальнена функція довіри ψ_a може бути представлена у такому вигляді:

$$\psi_a = f\left(\frac{\varphi_p}{R_p}; \frac{\varphi_{кс}}{R_{кс}}; \frac{\varphi_{ма}}{R_{ма}}\right), \tag{3.2}$$

де φ_p - безрозмірний показник якості результату реєстрації нового суб'єкта доступу;

$\varphi_{кс}$ - безрозмірний показник захищеності автентифікуючої інформації (конфіденційності секрету);

$\varphi_{ма}$ - безрозмірний показник коректності реалізації методу аутентифікації.

R_p - величина сумарного відносного ризику під час реєстрації;

$R_{кс}$ - величина сумарного відносного ризику при генерації, зберіганні,використанні та утилізації конфіденційності секрету;

$R_{ма}$ - величина відносного сумарного ризику під час реалізації методу аутентифікації.

Узагальнена функція довіри за визначенням може змінюватися в межах $0 \leq \varphi_a \leq 1$. Пояснимо фізичний сенс цієї функції. Чим ближче значення φ до одиниці, тим більша впевненість у достовірності, надійності та безпеці отриманих результатів аутентифікації суб'єкта доступу.

3.7 Формування рівнів довіри до автентифікації

Як було показано в першому розділі, міжнародні стандарти рекомендують введення принаймні трьох рівнів довіри до аутентифікації. Нагадаємо, що процес аутентифікації під час доступу суб'єкта до об'єкта має включати дії з перевірки автентичності суб'єкта доступу, а також приналежності йому пред'явленого ідентифікатора та аутентифікаційної інформації. Метою аутентифікації є формування необхідної впевненості в тому, що суб'єкт (об'єкт) доступу дійсно є тим зареєстрованим суб'єктом (об'єктом), за кого себе видає. Доведення автентичності суб'єкта доступу повинно ґрунтуватися на перевірці відповідності автентифікаційної інформації, пред'явленої суб'єктом, з автентифікаційною інформацією, що асоційована з пред'явленим ідентифікатором доступу в довіряючої сторони. Доведення приналежності суб'єкту ідентифікатора та автентифікаційної інформації повинно ґрунтуватися на перевірці актуальності (дійсності) автентифікаційної інформації та зв'язку ідентифікатора й автентифікаційної інформації із суб'єктом доступу.

З урахуванням вищевикладеного, методика формування рівнів довіри до результатів аутентифікації може бути представлена у вигляді таблиці 3.3.

У підсумку встановлено, що довіра до результатів автентифікації визначається досягнутою довірою до первинної ідентифікації суб'єкта доступу під час реєстрації, довірою до забезпечення конфіденційності секрету (автентифікуючої інформації) впродовж усього його життєвого циклу, а також довірою до коректності реалізації методів автентифікації, що включають організацію обміну автентифікаційною інформацією між заявником і сервером автентифікації (однобічний або взаємний обмін), використовувані при цьому фактори автентифікації та протоколи обміну.

На підсумковий рівень довіри істотно впливає співвідношення рівнів довіри до результатів ідентифікації та автентифікації (таблиця 3.4).

Таблиця 3.3 - Принципи формування рівнів довіри до аутентифікації

Метод автентифікації суб'єкта (об'єкта) доступу			Вид автентифікації суб'єкта (об'єкта) доступу	Упевненість, що суб'єкт та/або об'єкт доступу дійсно є тим, за кого себе видає	Рівень довіри до результатів автентифікації суб'єкта (об'єкта) доступу
Однофакторна аутентифікація	Одностороння аутентифікація	Відповідні протоколи аутентифікації, зокрема криптографічні	Проста	Деяка впевненість	Низький рівень довіри
Багатофакторна аутентифікація	Одностороння або взаємна аутентифікація	Відповідні протоколи аутентифікації, зокрема криптографічні	Посилена	Помірна впевненість	Середній рівень довіри
Багатофакторна аутентифікація	Взаємна автентифікація	Криптографічні протоколи аутентифікації	Строга	Значна впевненість	Високий рівень довіри

Таблиця 3.4 - Співвідношення рівнів довіри до результатів аутентифікації та ідентифікації

Рівень довіри до результатів аутентифікації	Рівень довіри до результатів ідентифікації		
	низький рівень довіри до результатів ідентифікації	середній рівень довіри до результатів ідентифікації	високий рівень довіри до результатів ідентифікації
1	2	3	4
Низький рівень довіри до результатів аутентифікації	Низький рівень довіри	Низький рівень довіри	Низький рівень довіри

Продовження таблиці 3.4

1	2	3	4
Середній рівень довіри до результатів аутентифікації	Низький рівень довіри	Середній рівень довіри	Середній рівень довіри
Високий рівень довіри до результатів аутентифікації	Низький рівень довіри	Середній рівень довіри	Високий рівень довіри

Зазначені рівні довіри мають узгоджуватися між собою. Пояснимо це на простому прикладі. Якщо для певних транзакцій застосовують сувору взаємну багатофакторну автентифікацію та автентифікаційну інформацію достатньо захищено, але реєстрацію нового користувача проводять тільки за копією паспорта, підсумковий рівень довіри до результатів ІА практично дорівнює нулю.

ВИСНОВКИ

1. Здійснено огляд та аналіз нормативно-правових документів, які регламентують процеси ідентифікації та аутентифікації, що дозволило розробити методику формування рівнів довіри.

2. На основі запропонованої методики розроблено класифікацію засобів та систем автентифікації суб'єктів доступу, що дозволило змоделювати процеси аутентифікації для дослідження надійності та безпеки її результатів.

3. На основі основних характеристик процесу аутентифікації суб'єктів доступу розроблено інфраструктуру довіри під час аутентифікації, що дозволило оцінити рівні довіри до результатів аутентифікації.

4. Розроблено алгоритми для формування рівнів довіри до методів аутентифікації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Global Internet Phenomena Report – Asia pacific, Africa and the middle-east. Sandvine inc. 2016. URL: https://www.sandvine.com/ resources/global-internet-phenomena/2016/asia pacific-africa-and-the-middle-east.html.
2. Кладій Ю.М., Максим'юк А.І., Осадчук О.Й., Скриник В.Я. Алгоритм ідентифікації мережевого трафіку та його тестування. Збірник матеріалів проблемної наукової міжгалузевої конференції «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ-2021). Тернопіль, 2021. С.11-12.
3. Волокітін А.В., Маношкин А.П., Солдатенков А.В., Савченко С.А., Петров Ю.А. Інформаційна безпека державних організацій і комерційних фірм. К.: Юніор, 2012. 303 с.
4. Інформаційна безпека: навчальний посібник. Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.
5. Authentication using the Google APIs Client [Електронний ресурс] – Режим доступу до ресурсу: https://developers.google.com/api-clientlibrary/javascript/start/start-js.
6. Dominic, Ehiwe & Kayode, Akinola & Ominike, Akpovi. (2018). Social Network Application User Authentication: 2FA with Encrypted Image. American Journal of Computing and Engineering Vol.3, Issue 1 No.1, pp 1 – 10
7. Features [Електронний ресурс] // authy. – 2019. – Режим доступу до ресурсу: https://authy.com/features/.
8. Electronic Identification, Authentication and Trust Services: EU Regulaton 910/2014 of 23 July 2014 eIDAS [Electronics resource]. Access mode: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.
9. Chapmen N., Chapman J. Authentication and Authorization on the Web, 2012. 246 p.

10. Mangard S., Oswald E., Popp T. Power Analysis Attaks: Revealing the Secrers of Smart Card. [USA]: Springer US, 2017. 338 p.

11. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. К.: КПІ ім. Ігоря Сікорського, 2018. 162 с. Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf

12. Akkar M., Giraud C. Koç Ç.K., Naccache D., Paar C. An implementation of DES and AES secure against some attacks. Cryptographic Hardware and Embedded Systems — CHES 2001. CHES 2001. Lecture Notes in Computer Science. 2001. Vol. 2162. P. 309-318.

13. Alshammari R., Zincir-Heywood A.N. An Investigation on the Identification of VoIP traffic: Case study on Gtalk and Skype. International Conference on Network and Service Management (CNSM). 2010. С. 310– 313.

14. OATH Certification [Електронний ресурс] // OATH Authentication. – 2019. – Режим доступу до ресурсу: https://openauthentication.org/oathcertification/.

15. Open source version of Google Authenticator [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/google/google-authenticator.

16. Segoro, Mauli & Putro, Prasetyo. (2020). Implementation of Two Factor Authentication (2FA) and Hybrid Encryption to Reduce the Impact of Account Theft 6 on Android-Based Instant Messaging (IM) Applications. 115-120. DOI:10.1109/IWBIS50925.2020.9255501.

17. The State of Strong Authentication [Електронний ресурс] // Javelin Strategy & Research. 2019. Режим доступу до ресурсу: https:// 1nmqmp2u9dgf3jo9centu6rq-wpengine.netdna-ssl.com/wpcontent/uploads/2019/01/ The-State-of-Strong-Authentication-2019-Report.pdf

18. ISO/IEC 24760-1:2011. Information technology — Security techniques – A framework for identity management – Part 1: Terminology and concepts [Електронний ресурс]: Geneva, Switzerland, International Organization for Standardization, [2011]. Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-1:v1:en.

19. ISO/IEC 29115:2013. Information technology – Security techniques – Entity authentication assurance framework [Електронний ресурс Geneva, Switzerland, International Organization for Standardization, [2013]. Режим доступу: http://www.iso.org/iso/catalogue_detail.htm?csnumber=45138.

20. ISO/IEC 24760-3:2016. Information technology – Security techniques – A framework for identity management – Part 3: Practice [Електронний ресурс]. Geneva, Switzerland, International Organization for Standardization, [2016]. Режим доступу: https://www.iso.org/standard/57916.html.

21. Lindeman R. Scalable authentication [Electronics resource]. Access mode: https://fidoalliance.org/specifications/additionalresources/.

22. FIDO. The State of Strong Authentication 2019. Adoption Rises under Threat of New Risks and Regulation. Javeling [Electronics resource]. Access mode: https://fidoalliance.org/specifications/download/.

23. Йовбак А.П., Марків А.П., Касянчук М.В. Огляд сучасних міжнародних стандартів для регламентації процесів аутентифікації. Збірник матеріалів науково - практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ-2023), Тернопіль, 2023. С.136-138.

24. Йовбак А.П., Осадчук О.Й., Касянчук В.М. Моделювання процесу аутентифікації для дослідження її надійності та безпеки інформації. Матеріали науково-практичного симпозіуму «Захист інформації». Тернопіль, 2023. С.78-82.

25. ISO/IEC 29146: 2016 Information technology – Security techniques – Framework for Access Control. URL: https:// www.iso.org/ru/standard/45169.html

26. ISO/IEC 29003: 2017 Information technology – Security techniques – Identity Proofing. URL: https://www.iso.org/ru/ standard/62290.html

27. FIPS 196, "Entity authentication using public key cryptography" Federal Information Processing Standards Publication, U.S. Department of Commerce / N.I.S.T., National Technical Information Service, Springfield, Virginia, 1997 [Electronics resource]. Access mode: http://csrc.nist.gov/publications/fips/fips196/fips196.pdf.

28. ITU-T Rec.X.1254 (09/2012): Geneva, Switzerland, International Telecommunication Union, [2012]. Режим доступа: https://www.itu.int/rec/T-REC-X.1254-201209-I/en.

29. ITU-T Rec.X.1255 (09/2013. Geneva, Switzerland, International Telecommunication Union, [1988]. Режим доступу: https://www.itu.int/rec/T-REC-X.1255-201309-I.

30. Остапов С. Технології захисту інформації. Посібник. Родовід, 2014. 428 с.

31. Nykolaychuk Ya.M., Kasianchuk M.M., Yakymenko I.Z. Symmetric Cryptoalgorithms in the Residue Number System. Cybernetics and Systems Analysis. Springer US, is. 52, 2021. PP. 219-223.

ДОДАТОК А

Копії публікацій