МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

Гулька Олександр Олександрович

Алгоритми захисту персональних даних пацієнта в телемедицині / Algorithms for patient data protecting in telemedicine

спеціальність:123 – Комп'ютерна інженерія
освітньо-професійна програма – Комп'ютерна інженерія

Випускна кваліфікаційна робота

Виконав студент групи КІм-21
О. О. Гулька
_____

Науковий керівник:
к.т.н., Дубчак Л.О.
_____

ТЕРНОПІЛЬ - 2019

РЕЗЮМЕ

Магістерська робота на тему “Алгоритми захисту персональних даних пацієнта в телемедицині” на здобуття освітньо-кваліфікаційного рівня “Магістр” зі спеціальності “Комп’ютерні системи та мережі” написана обсягом 73 сторінок і містить 14 ілюстрацій, 3 таблиці, 3 додатки та 50 джерел за переліком посилань.

Метою даної роботи є розробка політики безпеки телемедичної системи.

Об’єктом досліджень є система захисту інформації в телемедицині. Предметом досліджень є алгоритми захисту персональних даних пацієнта в телемедицині.

Методи проведених досліджень – симетричні та асиметричні методи захисту інформації, нечіткі методи обробки інформації.

Наукова новизна полягає у вдосконаленні алгоритму вибору криптоалгоритму обробки персональної інформації пацієнта в телемедицині, що базується на нечіткій логіці.

Здійснено аналіз аналіз даних в телемедичній системі, що дозволило розробити основні підходи до їх захисту. Розроблено основні підходи до управління доступом до конфіденційної інформації телемедицини, що дась можливість розробки адекватної політики захисту.

Здійснено розробку та верифікацію нечіткої системи вибору алгоритму захисту інформації в телемедичній системі, що дозволить реалізувати політику захисту залежно від поточного стану системи, даних, що захищаються, та відповідно до поточного користувача телемедицини.

КЛЮЧОВІ СЛОВА: КРИПТОАЛГОРИТМ, ТЕЛЕМЕДИЦИНА, ПОЛІТИКИ ЗАХИСТУ, НЕЧІТКА СИСТЕМА.

RESUME

The master's thesis on " Algorithms for patient data protecting in telemedicine " for obtaining the master's qualification level in the specialty "Computer systems and networks" is written with a volume of 73 pages and contains 14 illustrations, 3 tables, 3 supplements and 50 sources for a list of links.

The purpose of this work is to develop a security policy for the telemedicine system.

The subject of the research is the telemedicine information security system. The subject of research is algorithms for protection of patient's personal data in telemedicine.

Research methods are symmetrical and asymmetric methods of information protection, fuzzy methods of information processing.

The scientific novelty is to improve the algorithm for selecting a crypto algorithm for processing personal information of a patient in telemedicine based on fuzzy logic.

An analysis of data analysis in the telemedicine system was performed, which allowed to develop basic approaches to their protection. Basic approaches to the management of access to confidential telemedicine information have been developed, which in turn gives the opportunity to develop an adequate protection policy.

A fuzzy system for selecting the information security algorithm for the telemedicine system has been developed and verified, which will allow implementation of a security policy depending on the current state of the system, the protected data and according to the current telemedicine user.

KEYWORDS: CRYPTOALGORITHM, TELEMEDICINE, PROTECTION POLICIES, FUZZY SYSTEM.

ЗМІСТ

Вступ 11
1 Сучасний стан захисту інформації в телемедицині 14
1.1 Телемедицина в Україні 14
1.2 Політика захисту інформації в телемедичних системах 23
1.3 Аналіз завдання та постановка задачі 31
2 Розробка політики захисту конфіденційної інформації в телемедичній системі .. 34
2.1 Дані в телемедичній системі, які потребують захисту 34
2.2 Алгоритми управління доступом до конфіденційної інформації телемедицини 35
2.3 Застосування нечіткої логіки в задачах захисту інформації 46
3 Нечітка система вибору алгоритму шифрування 53
3.1 Загальна схема нечіткої системи 53
3.2 Реалізація нечіткої системи вибору алгоритму шифрування 57
3.3 Верифікація та тестування запропонованої нечіткої системи 60
3.4 Апаратна реалізація нечіткої системи захисту інформації в телемедицині 63
Висновки 72
Список використаних джерел 73
Додаток А MATLAB код нечіткої системи вибору криптоалгоритму 78

ВСТУП

Актуальність досліджень. Розвиток інформаційних технологій наклало свій відбиток і на розвиток медицини. З'явилася можливість проводити консультації провідних фахівців не залежно від їх місця знаходження, контролювати процес лікування пацієнта, здійснювати керування проведенням хірургічних операцій, надавати психологічну допомогу і т.д.

Телемедицина – це сучасний напрям розвитку інформатизації медицини, який передбачає використання сучасних інформаційних та телекомунікаційних технологій для дистанційної діагностики та лікування захворювань, надання допомоги в надзвичайних та екстренних ситуаціях, підвищення кваліфікації медичних працівників [1].

Згідно наказу МОЗ України №681 головною метою телемедицини є поліпшення здоров'я населення шляхом забезпечення рівного доступу до медичних послуг належної якості [2].

Основними завданнями телемедицини є:

- забезпечення надання медичної допомоги пацієнту, коли відстань є критичним чинником її надання;
- збереження медичної таємниці та конфіденційності, цілісності медичної інформації про стан здоров'я пацієнта;
- створення єдиного медичного простору;
- сприяння підвищенню якості допомоги та оптимізації процесів організації та управління охороною здоров'я;
- формування системних підходів до впровадження та розвитку телемедицини в системі охорони здоров'я.

З поняттям телемедицини тісно пов'язана телемедична мережа, тобто форма організації надання медичної допомоги населенню із застосуванням

телемедицини.

Телемедична мережа дає змогу:

- упорядкувати та систематизувати процес надання медичної допомоги із застосуванням телемедицини;
- забезпечити сумісність інформації та даних при наданні медичної допомоги із застосуванням телемедицини;
- забезпечити використання медичних інформаційних стандартів у процесі надання медичної допомоги із застосуванням телемедицини;
- здійснювати контроль якості надання медичної допомоги із застосуванням телемедицини.

Сукупність усіх технологій, що дають змогу проводити дистанційне вимірювання, збір і передачу інформації про показники діяльності (фізіологічні параметри) організму пацієнта називається телеметрією [1].

Сучасні системи автоматизованої мікроскопії локальні, а при постановці діагнозу дуже часто залучаються медичні експерти з різних галузей та країн світу. Телемедицина є найоптимальнішим шляхом швидкої і правильної постановки діагнозу, що особливо актуально в онкології. Тому виникає необхідність розробки онкотелемедицини, яка працює в реальному часі і забезпечує захист медичної інформації.

Метою даної роботи є розробка політики безпеки телемедичної системи.

Для досягнення мети необхідно вирішити наступні **задачі**:

1) здійснити аналіз сучасних телемедичних систем;
2) провести дослідження основних модулів телемедицини;
3) проаналізувати сучасні алгоритми захисту інформації;
4) аргументувати вибір алгоритму захисту конфіденційної інформації в телемедицині;
5) вибрати шлях реалізації алгоритму, зокрема можливість застосування апарату нечіткої логіки;
6) розробити нечітку систему вибору алгоритму захисту інформації;

7) здійснити реалізацію розробленої системи;

8) провести симуляцію змодельованого засобу захисту.

Об'єктом досліджень є система захисту інформації в телемедицині.

Предметом досліджень є алгоритми захисту персональних даних пацієнта в телемедицині.

Методи проведених досліджень – симетричні та асиметричні методи захисту інформації, нечіткі методи обробки інформації.

Наукова новизна полягає у вдосконаленні алгоритму вибору криптоалгоритму обробки персональної інформації пацієнта в телемедицині, що базується на нечіткій логіці.

Практичне значення одержаних результатів полягає у розробленому нечіткому контролері, що працює в реальному часі і може застосовуватися у будь-якій телемедичні системі та швидко переналаштовуватись.

Публікації та апробації результатів досліджень здійснено на I та II науково-практична конференція молодих вчених і студентів «Інтелектуальні комп'ютерні системи та мережі», м.Тернопіль, 2019 р. (додаток Б).

Впровадження результатів досліджень здійснено в лікувальному кабінеті (додаток В).

Випускна кваліфікаційна робота складається з трьох розділів [3, 4].

В **першому розділі** здійснено аналіз сучасного стану телемедицини в Україні та світі. Крім того, досліджено алгоритми захисту конфіденційної інформації та виділено найстійкіші для побудови системи захисту особистої інформації пацієнта.

В **другому розділі** розроблено нечітку систему вибору криптоалгоритму захисту інформації, використовуючи ризик виникнення атаки та рівень доступу клієнта. Проведено її моделювання та дослідження роботи.

В третьому розділі розроблено та здійснено симуляцію роботи нечіткого контролеру вибору крипто алгоритму для подальшого його застосування в телемедичних системах.

1 СУЧАСНИЙ СТАН ЗАХИСТУ ІНФОРМАЦІЇ В ТЕЛЕМЕДИЦИНІ

1.1 Телемедицина в Україні

Розвиток інформаційних технологій наклало свій відбиток і на розвиток медицини. З’явилася можливість проводити консультації провідних фахівців не залежно від їх місця знаходження, контролювати процес лікування пацієнта, здійснювати керування проведенням хірургічних операцій, надавати психологічну допомогу і т.д.

Сьогодні існує підвищена тенденція до розвитку телемедицини, оскільки вона широко розглядається як ресурс, здатний революціонізувати доступ до медичних послуг. Найважливіші сфери ефективного використання телемедицини: телеконсультації, теледіагностика, телемедицина, теленавчання, телепрограмування, телемоніторення і телепідтримка. Окрім незаперечної переваги телемедицини, існує ще багато проблем та етичних питань, які потрібно вирішити. Проте телемедицина стає частиною нашого життя, і її значення в системі охорони здоров'я зростає [1].

Одним з основних завдань телемедицини є швидке діагностування невідкладних станів у пацієнтів, тому необхідною є розробка нових методів та засобів, що допомагають лікареві у своєчасній постановці діагнозу.

Рак молочної залози є однією з найбільших проблем сучасних жінок. Постановка такого діагнозу відбувається на основі аналізу гістологічних та цитологічних зображень, які опрацьовує лікар. Проте завжди існує ризик лікарської помилки чи інших суб’єктивних причин неправильного чи несвоєчасного діагнозу. Тому розробка автоматизованої системи аналізу таких зображень, яка є складовою телемедичних комплексів, є актуальною задачею.

Багато науковців застосовують методи штучного інтелекту для розробки нових систем діагностування, зокрема апарат нечіткої логіки.

Використовуючи комунікаційні технології, покращуються методи швидкого і кращого діагностування та методів надання медичної допомоги. Швидкі зв'язки між лікарями та пацієнтами здійснюються завдяки вдосконаленню телемедичних технологій. Наприклад, у дослідженні [2] розроблено новий метод діагностики травмованої селезінки за наявності розриву, контузії, активної кровотечі або гематоми через травму черевної порожнини, використовуючи телемедицину на основі таблеток. Клініцисти повідомляли електронною поштою та діагностували патологічні результати, які належать 10 пацієнтам. Завдяки більш швидкій діагностиці запропонована авторами система зменшує смертність і захворюваність невідкладних пацієнтів.

Телемедицина – це сучасний напрям розвитку інформатизації медицини, який передбачає використання сучасних інформаційних та телекомунікаційних технологій для дистанційної діагностики та лікування захворювань, надання допомоги в надзвичайних та екстренних ситуаціях, підвищення кваліфікації медичних працівників [1].

Згідно наказу МОЗ України №681 головною метою телемедицини є поліпшення здоров’я населення шляхом забезпечення рівного доступу до медичних послуг належної якості.

Основними завданнями телемедицини є [1]:

– забезпечення надання медичної допомоги пацієнту, коли відстань є критичним чинником її надання;

– збереження медичної таємниці та конфіденційності, цілісності медичної інформації про стан здоров’я пацієнта;

– створення єдиного медичного простору;

– сприяння підвищенню якості допомоги та оптимізації процесів організації та управління охороною здоров’я;

– формування системних підходів до впровадження та розвитку телемедицини в системі охорони здоров’я.

З поняттям телемедицини тісно пов’язана телемедична мережа, тобто форма організації надання медичної допомоги населенню із застосуванням телемедицини.

Телемедична мережа дає змогу:

– упорядкувати та систематизувати процес надання медичної допомоги із застосуванням телемедицини;

– забезпечити сумісність інформації та даних при наданні медичної допомоги із застосуванням телемедицини;

– забезпечити використання медичних інформаційних стандартів у процесі надання медичної допомоги із застосуванням телемедицини;

– здійснювати контроль якості надання медичної допомоги із застосуванням телемедицини.

Сукупність усіх технологій, що дають змогу проводити дистанційне вимірювання, збір і передачу інформації про показники діяльності (фізіологічні параметри) організму пацієнта називається телеметрією [1].

Сучасні системи автоматизованої мікроскопії локальні, а при постановці діагнозу дуже часто залучаються медичні експерти з різних галузей та країн світу. Телемедицина є найоптимальнішим шляхом швидкої і правильної постановки діагнозу, що особливо актуально в онкології. Тому виникає необхідність розробки онкотелемедицини, яка працює в реальному часі і забезпечує захист медичної інформації.

Згідно досліджень, проведених у [2], темпи зростання ринку телемедицини зростає на 18-30% в рік. Загальний річний дохід США у 2013 році становив $ 9,6 млрд. і прогнозується його зростання до $ 38,5 млрд. виручки до 2018 року.

37 % відсотків роботодавців в світі вже запропонували своїм працівникам телемедичні послуги.

Згідно з даними опитування, проведеного Intel, 72 % споживачів сказали, що вони готові звернутися до лікаря за допомогою телемедицини при не ургентних станах. Три відомі альянси членів Connected Care, Anthem, MD Live і

Teladoc вже повідомляють про задоволеність телемедициною пацієнтів більше, ніж на 95 % [2].

Споживачі послуг охорони здоров'я вимагають зручний та високоякісни догляд і телемедицина пропонує його.

Початок розвитку телемедицини в Україні пов’язують з 1940-ми роками, а саме з дослідженнями, які проводилися в рамках космічних проектів. Після цього здійснювався розвиток, в основному, передачі ЕКГ по різних каналах зв’язку та відеоконсультування.

В 1994 році відбулися переговори з міжнародними фахівцями з впровадження телемедицини в Україні та здійснилися перші телеконсультації. З кінця 1990-х років розвивалася національна мережа теле-ЕКГ. В 2000 році створився перший в Україні телемедичний центр (в Донецкому НДІ травматології та ортопедії). Пізніше телемедицина почала впроваджуватися в клінічну роботу в ряді областей країни (телетравматологія і телеортопедія, теледерматологія, телерадіологія).

Обласні телемедичні мережі функціонують з 2002 року. У 2006 році створилася національна громадська організація – Асоціація розвитку української телемедицини та електронної охорони здоров'я [3].

В Україні у 2007 році створено Державний клінічний науково-практичний центр телемедицини МОЗ України — єдиний спеціалізований заклад охорони здоров'я, створений для впровадження та розвитку телемедицини в Україні. Згідно Статуту, він забезпечує надання висококваліфікованої комплексної консультативної медичної допомоги населенню із застосуванням телемедичних технологій. Із 2009 року Державним центром телемедицини реалізується проект створення телемедичної мережі України, завдяки якій започатковано телемедичне консультування та обмін досвідом лікарів.

На даний час відбувається бурхливий розвиток і швидке впровадження телемедицини по всіх країнах світу.

У розвинутих країнах телемедицина вже працює на повну силу. Однак для України цей вид надання медичної допомоги належить до технологій, які тільки-но почали впроваджувати в практику. Процес іде досить повільно, бо для цього потрібні, насамперед, значні кошти. Втім, як показує зарубіжний досвід, вкладені сьогодні в розвиток телемедицини гроші окупляться сторицею в майбутньому.

Ззапровадження телемедицини в Україні почали дбати ще 12 років тому, коли було створено ДЗ «Медичний центр телемедицини МОЗ України». Однак відтоді вдалося зробити небагато, та й те, що було реалізовано, на оплески навряд чи заслуговує, оскільки все відбувалося дуже повільно й в окремих регіонах. Потім було прийнято Наказ від 26.03.2010 р. №261 «Про впровадження телемедицини в закладах охорони здоров'я», яким було затверджено ряд нормативних документів. Проте тоді зробити щось конкретне в плані реального запровадження телемедицини вдалося лише за підтримки бізнесу та благодійних організацій. Зокрема, протягом 2012-2014 років на це спромоглися лише 9 закладів охорони здоров'я зі Львівської, Дніпропетровської та Донецької областей завдяки реалізації положень Меморандуму про взаєморозуміння між МОЗ України, НАМН України, ТОВ «ДТЕК», БФ «Розвиток України» та ПрАТ «МТС Україна», підписаного у 2011 році.

Наступний крок зроблено у жовтні 2015 року: МОЗ України видало Наказ №681 «Про затвердження нормативних документів щодо застосування телемедицини у сфері охорони здоров'я», в якому було прописано Порядок організації медичної допомоги на первинному, вторинному (спеціалізованому), третинному (високоспеціалізованому) рівнях із застосуванням телемедицини, Положення про кабінет телемедицини закладу охорони здоров'я та форми первинної облікової документації.

І лише у 2017-му з'явилися перші результати запровадження телемедицини на державному рівні: сільські лікарі та фельдшери Одещини отримали змогу дистанційно передавати до обласних лікувальних закладів

кардіограми пацієнтів та отримувати консультації фахівців. Це стало можливим завдяки забезпеченню медиків первинки спеціальними мобільно-діагностичними сумками-укладками, куди входять камера-USB, електрокардіограф, глюкометр, ендоскоп, спірометр, тонометр тощо, підключені до планшета. Однак тоді до пілотного проекту потрапили лише два заклади: КНП «Окнянська цетральна районна лікарня» й амбулаторії КНП «Окнянський районний центр первинної медико-санітарної допомоги», але телемедичні консультації проводилися виключно хворим із серцево-судинними недугами.

Уже сьогодні понад 24 млн українців отримали доступ до гарантованого пакету послуг, які надають сімейні лікарі, терапевти та педіатри, а оплачує Національна служба здоров'я.

Менш ніж за 9 місяців медичним закладам первинного рівня вдалося провести масову комп'ютеризацію. За даними обласних ДОЗ, майже 97% закладів первинки вже обладнані необхідно технікою. Це важливі передумови для розвитку телемедицини, адже з'явилася технічна можливість обробляти телемедичні дані.

Нагадаємо, в Україні розпочалося будівництво перших 517 нових сільських амбулаторій. 10 вже введено в експлуатацію на Кіровоградщині. Спільно з МОЗ, розроблено і сформовано спроможну мережу з 4223 сільських амбулаторій.

Загальна схема телемедицини подана на рисунку 1.1.

Рисунок 1.1 – Загальна схема телемедицини

Зважаючи на значне поширення телемедицини останнім часом в світі та її розвиток в Україні можна виділити наступні основні проблеми, які потребують вирішення при впровадженні.

Перш за все важливою є відповідність телемедицини юридичним законам. Проте, на даний час існує плутанина щодо її юридичного регулювання в різних країнах світу. В Україні при впровадженні телемедицини необхідно слідувати наказу МОЗ України №681 та ДСТУ України щодо захисту інформації [1].

Наступна проблема стосується апаратного та програмного забезпечення телемедицини. Зокрема, необхідно враховувати їх вартість, тобто вони повинні бути економічно вигідними не тільки для комерційних, а й для державних лікувальних закладів. Крім того, програмно-апаратні засоби повинні мати простий інтерфейс для користувачів, зокрема лікарів та пацієнтів.

Варто зазначити, що програмне та апаратне забезпечення вибирається в залежності від задач, які розв'язує телемедицина (наприклад, необхідність опрацювання зображень в онкології або проведення відеозв'язку при проведенні онлайн операцій і т.д.).

Сучасний етап розвитку інформаційних управляючих систем (ІУС) характеризується підвищеними вимогами до якості функціонування. Проте, не дивлячись на інтенсивний розвиток і впровадження сучасних технологій і методів, що застосовуються при створенні інформаційних управляючих систем, в даній області залишаються ще не вирішені задачі. Підвищену увагу до проблем якості ІУС спричиняє важливість функцій, які виконуються системою і, як наслідок цього, зростають вимоги до надійності та якості їх виконання в реальних умовах експлуатації.

Вирішення проблеми забезпечення та підвищення якості інформаційних управляючих систем має багато напрямів. Одним із них є моніторинг факторів впливу на надійність ІУС, результати якого дають змогу виявити та врахувати недоліки проектування складових частин системи.

Іншим підходом може бути врахування зміни надійності найбільш впливаючих факторів в процесі експлуатації та, як наслідок, зміни рівня якості функціонування системи з метою оперативного втручання в роботу системи та прийняття рішень щодо втримання системи на заданому рівні якості

функціонування. До переліку впливаючих факторів можливого погіршення функціонування системи, спричиненого її забезпечуючою частиною, рекомендується вносити технічну, програмну та інформаційну складові [1, 2].

Ці характеристики необхідно враховувати при розробці нових чи виборі вже існуючих апаратних та програмних засобів.

Захисту інформації при експлуатації телемедицини присвячено багато досліджень. Зокрема, для захисту персональних даних пацієнта пропонують застосовувати різні криптоалгоритми, а для підтвердження діагнозу чи переданої інформації лікарем-консультантом пропонується застосовувати електронний цифровий підпис [4]. Деякі науковці для захисту зображень застосовують водяні знаки. Проте, варто зазначити, що політика безпеки повинна розроблятися у кожному конкретному випадку впровадження телемедицини [5-7].

Однією з найменш досліджених задач є вибір експертів для проведення консультацій. В літературі зазначається, що лікар-консультант повинен бути висококваліфікованим та практикувати у відповідній галузі медицини. Проте, необхідно враховувати, що думка експерта є суб'єктивною і інколи діагноз, поставлений ним, може не відповідати дійсності.

Дану проблему можна вирішити за допомогою апарату нечіткої логіки, враховуючи усі правильні і неправильні діагності, поставлені конкретним консультантом, а також можливість виникнення несанкціонованого доступу до інформації при проведенні ним консультацій.

Отже, в загальному при впровадженні телемедицини в експлуатацію необхідно вирашити наступні задачі:

1) визначення напрямку медичних консультацій при застосуванні телемедицини;

2) вибір юридичної бази;

3) розробка політики безпеки з визначенням учасників телемедицини, розподілу їх прав та відповідних криптографічних засобів захисту інформації;

4) вибір або розробка нових апаратних та програмних засобів з врахуванням визначених вище характеристик;

5) розробка системи вибору експертів;

6) тестування та верифікація створеної телемедицини.

Для розробки працездатної онкотелемедицини необхідно врахувати всі зазначені вище проблеми та вибрати найоптимальніші шляхи їх вирішення.

1.2 Політика захисту інформації в телемедичних системах

Телемедицина поділяється на локальну та глобальну. В глобальній медичній консультативно-діагностичній системі в ролі клієнта виступають підсистеми консультативно-діагностичних пунктів чи центрів, а сервер виконує роль накопичувача та координаційно-технічного центру [2].

Будь-яка інформаційна система включає [2]: прикладне програмне забезпечення (ППЗ), яке відповідає за зв’язок системи з клієнтом; системи управління базами даних (СУБД); операційну систему для обслуговування ППЗ та СУБД; мережу, яка забезпечує взаємодію всіх вузлів інформаційної системи.

Найнебезпечнішими для таких інформаційних систем є:

- несанкціонований доступ до паролей чи конфіденційної інформації,
- порушення прав доступу,
- атаки типу «відмова в обслуговуванні»,
- «пряма» атака,
- віруси,
- сучасні атаки по побічних каналах витоку інформації.

Несанкціонований доступ полягає у підборі чи викраденні пароля або підміні IP-адреси законного користувача системи. До цього виду атак вразливі усі компоненти інформаційної системи.

Існує чотири стандартні підходи, за допомогою яких можна обмежити доступ до інформації, а саме контроль доступу, розширення парольного захисту, шифрування даних та використання брандмауерів [3].

Атака типу «відмова в обслуговуванні» полягає у створенні неправильного пакету даних чи передачі великої кількості пакетів даних по мережі з метою блокування роботи контролера домена, що зупиняє роботу комп’ютерної системи. Для захисту компонентів інформаційної системи застосовуються спеціальні програми виявлення такого типу атак чи міжмережеві екрани [4].

Комп'ютерний вірус – комп'ютерна програма, яка має здатність до прихованого саморозмноження. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера. Розрізняють файлові, завантажувальні та макро-віруси або комбінації цих типів. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу. Для захисту від вірусів на даний час існує багато антивірусних програм, що захищає інформаційну систему від пошкодження.

Побічними каналами витоку інформації під час передачі пакетів даних по мережі є електро-магнітне випромінювання, час виконання алгоритмів шифрування та реакція системи на спеціально внесені помилки. Для протидії таким атакам використовуються, як правило, архітектурна та операційна надлишковість, тобто додаткові апаратні та програмні засоби [3, 5].

Загалом можна визначити наступні методи захисту інформаційної системи від втрати чи викриття конфіденційної інформації [2].

Установка перешкоди – метод фізичного перешкоджання шляху зловмиснику до інформації, що захищається, у тому числі спроб з використанням технічних засобів знімання інформації і дії на неї.

Маскування – метод захисту інформації з використанням інженерних, технічних засобів, а також шляхом криптографічного закриття інформації.

Управління доступом – метод захисту інформації за рахунок регулювання використовування всіх інформаційних ресурсів, у тому числі автоматизованої інформаційної системи підприємства. Управління доступом включає наступні функції захисту:

1) ідентифікацію користувачів, персоналу і ресурсів інформаційної системи (привласнення кожному об'єкту персонального ідентифікатора);

2) аутентифікацію (встановлення автентичності) об'єкта або суб'єкта після пред'явлення ними ідентифікатора;

3) перевірку повноважень (перевірка відповідності дня тижня, часу доби, запрошуваних ресурсів і процедур встановленому регламенту);

4) дозвіл і створення умов роботи в межах встановленого регламенту;

5) реєстрацію (протоколювання) звернень до ресурсів, що захищаються;

6) реагування (сигналізація, відключення, затримка робіт, відмова в запиті) при спробах несанкціонованих дій.

Проте, застосування всіх відомих методів захисту даних інформаційної системи не гарантує збереження цілісності даних, тому розробка нових підходів залишається актуальною задачею.

З метою побудови стійкої телемедичної системи, яка відповідає усім вимогам, запропоновано наступні складові політики безпеки.

1. Загальні вимоги до ОС та ПК:

– версія Windows 7/10 з метою шифрування диску, де знаходиться база даних чи система вцілому;

– наявність антивірусної та антишпигунських програм;

– база даних повинна знаходитись на сервері, що є недоступним користувачам системи, крім адміністратора;

– системний блок сервера опломбовується для запобігання підключення додаткових апаратних засобів зчитування і передачі інформації.

2. Вимоги до адміністрування:

а) рівні доступу і відповідні їм права:

– адміністратор – доступ до системи, програмних засобів (ПЗ), бази даних – має право надавати права і рівні доступу користувачам на певний час чи на постійно, вносити зміни в ПЗ чи базу даних, проводити аутентифікацію користувачів, а також перевірку і зміну політики безпеки;

– лікуючий лікар – доступ до системи через власний інтерфейс, доступ до бази даних, доступ до інформації про пацієнта, доступ до засобів відео- та аудіозв’язку, передача даних по мережі (за допомогою електронного цифрового підпису (ЕЦП) чи записом в журналі телемедицини, згідно наказу МОЗ №681) – має право обирати лікаря-консультанта, здійснювати аудіо- та відеозв’язок, вносити зміни в базу даних, передавати зашифровані дані про пацієнта, підтверджуючи їх за допомогою ЕЦП чи записом в журналі телемедицини, згідно наказу МОЗ №681;

– лікар-консультант – доступ до системи через свій інтерфейс, доступ до засобів відео- та аудіозв’язку, передача даних по мережі – має право доступу до даних, що передає лікуючий лікар, здійснювати запит на додаткову інформацію про пацієнта (крім прізвища та ім’я пацієнта), ставити діагноз та передавати його лікуючому лікареві, підтверджуючи його своїм ЕЦП записом в журналі телемедицини, згідно наказу МОЗ №681;

– пацієнт – доступ до системи через свій інтерфейс, подача особистих даних, зв'язок з лікуючим лікарем – має право здійснювати відео- та аудіозв’язк з лікуючим лікарем, подавати свою особисту інформацію, необхідну для постановки діагнозу, вимагати захисту своїх особистих даних від лікуючого

лікаря та адміністратора, вимагати підтвердження особи лікуючого лікаря під час передачі даних (через ідентифікацію чи ЕЦП);

– лаборант – доступ до системи через власний інтерфейс, внесення даних в базу даних з підтвердженням своєї особи (через ідентифікацію чи ЕЦП), передача та отримання повідомлень від лікуючого лікаря.

b) Проведення аутентифікації лікарів-консультантів:

– для підтвердження особи лікаря-консультанта адміністратор може вимагати документи, які підтверджують кваліфікацію лікаря, а також час від часу здійснювати, крім ідентифікації, аутентифікацію;

– при здійсненні доступу користувачів до системи повинна здійснюватись їх ідентифікація.

3. Захист бази даних:

– гістологічні зображення зберігаються під зашифрованими номерами, відповідно до особи пацієнта, в незміненому стані;

– вся інформація про пацієнта зберігається в зашифрованому вигляді;

– доступ до бази даних здійснюється через ідентифікацію, відповідно до прав доступу.

4. Передача даних по мережі:

– ідентифікація лікуючого лікаря та лікаря-консультанта перед здійсненням консультації та передачі даних;

– гістологічні зображення передаються по мережі або записуються на віртуальний диск в незміненому вигляді без вказання прізвища та імені пацієнта;

– необхідна додаткова інформація передається в зашифрованому вигляді за допомогою симетричного чи асиметричного криптоалгоритму;

– лікар-консультант пересилає свій діагноз та рекомендації щодо лікування через електронну пошту з підтвердженням за допомогою ЕЦП.

Враховуючи усі вказані вимоги можна розробити телемедичну систему, яка буде працездатною та стійкою до атак.

Інформаційні системи (ІС) різного масштабу стали невід'ємною частиною базової інфраструктури держави, бізнесу, громадянського суспільства. З кожним разом, все більше інформації, що захищається, переноситься в ІС.

Особливо увагу захисту інформації надається в медицині, зокрема в системах автоматизованої мікроскопії. Оскільки, у таких системах зберігається особиста конфіденційна інформація про користувачів системи та пацієнтів. Механізм розподілу прав доступу, авторизації та автентифікації є складовою успішного та надійного функціонування багатокористувацьких систем. Системи автоматизованої мікроскопії широко застосовуються для аналізу гістологічних та цитологічних зображень [5].

Актуальною є розробка алгоритму авторизації та автентифікації користувачів системи автоматизованої системи з подальшим розподілом прав доступу.

Основою будь-яких систем захисту інформаційних систем є ідентифікація і автентифікація, так як всі механізми захисту інформації розраховані на роботу з поіменованими суб'єктами і об'єктами.

В якості суб'єктів можуть виступати як користувачі, так і процеси, а в якості об'єктів - інформація та інші інформаційні ресурси системи. Присвоєння суб'єктам і об'єктам доступу особистого ідентифікатора і порівняння його з заданим переліком називається ідентифікацією.

Ідентифікація забезпечує виконання наступних функцій: встановлення автентичності та визначення повноважень суб'єкта про його допуск в систему, контролювання встановлених повноважень, реєстрація дій і т.д.

Модуль розроблений за шаблоном проектування MVC (Model-View-Controller). MVC побудований таким чином, що модифікація одного компоненту мінімально впливає на зміну будь-якого іншого. Це дозволяє змінювати певний клас без значних змін іншого або й взагалі без змін іншого класу.

Вікно для вводу даних користувача (логін та пароль) є стартовим для усієї системи. Модуль працює за наступним алгоритмом:

1) зчитування введених даних з форм вводу;
2) перевірка даних на коректність за допомогою регулярних виразів;
3) підключення до СУБД MySQL;
4) порівняння перевірених даних з еталоном (автентифікація);
5) надання доступу до системи та розподіл прав (авторизація).

Для шифрування пароля було використано алгоритм MD5 з додаванням "солі". MD5 є одним з алгоритмів шифрування на 128-бітної основі [7].

Під шифруванням розуміють перетворення вхідних даних за певним алгоритмом в бітовий рядок певної довжини.

При цьому отриманий в ході обчислень результат представлений в шістнадцятковій системі числення. Вона називається хешем, хеш-сумою або хеш-кодом [15]. Для кожного користувача, "сіль" є унікальним набором символів різної довжини. Тому, навіть при однакових паролях, хеш-сума буде різною.

Загальна процедура ідентифікації і автентифікації користувача при його доступі в систему представлена на рисунку 1.2.

Введені дані перевіряються наступним чином:

1) для введеного логіна (якщо такий існує) зчитується унікальний ключ;
2) відбувається конкатинація пароля з ключем;
3) отримана стрічка подається на вхід хеш-функції;
4) відбувається порівняння вихідної стрічки з паролем у базі;
5) в разі успіху відкривається головне вікно програми.

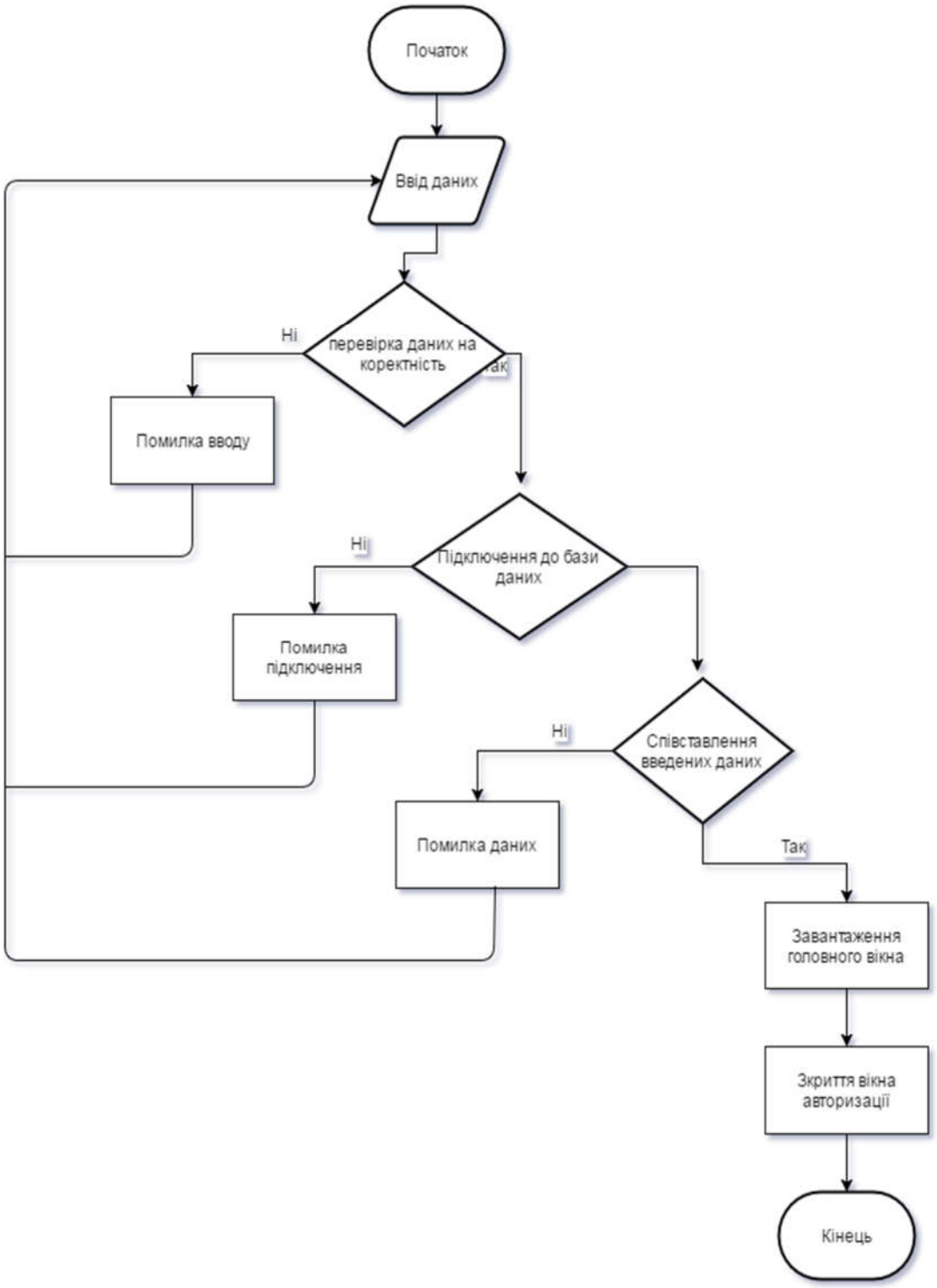


Рисунок 1.2 - Блок - схема роботи модуля авторизації

Якщо в процесі автентифікації справжність суб'єкта встановлена, то система захисту інформації повинна визначити його повноваження (сукупність прав). Це необхідно для подальшого контролю і розмежування доступу до ресурсів.

Переваги запропонованого підходу:

1) швидка інтеграція у будь-який Java FX додаток;
2) два ступені авторизації: автентифікація та надання прав доступу;
3) валідація введених даних у два кроки;
4) зручний інтерфейс користувача.

Застосування такого підходу до розробки системи автоматизованої мікроскопії в телемедицині дозволяє забезпечити зручний інтерфейс для користувачів, точність постановки діагнозу на основі цитологічних та гістологічних зображень та захист конфіденційної медичної інформації про пацієнта.

1.3 Аналіз завдання та постановка задачі

Розглянувши кілька базових атак, що можуть бути застосовані до сучасних засобів криптографічного захисту інформації, можна сказати, що зловмисник має дуже багато можливостей для анонімного здійснення успішної атаки на телемедичну систему.

Збільшення об’ємів, цінності та швидкості передачі інформації, яка пересилається комп’ютерними мережами та за допомогою Internet, зумовлює необхідність використання спеціалізованих засобів захисту інформації. На даний час найпопулярнішими є асиметричні алгоритми захисту інформації, розміщення бази даних на віддалених ресурсах і т.д.

Отже, актуальною задачею є розроблення політики захисту телемедицини, яка буде забезпечувати захист персональних даних пацієнтів та здійснювати правильний розподіл доступу персоналу до інформації в базі даних.

На рисунку 1.3 представлено процес постановки задачі магістерської роботи.

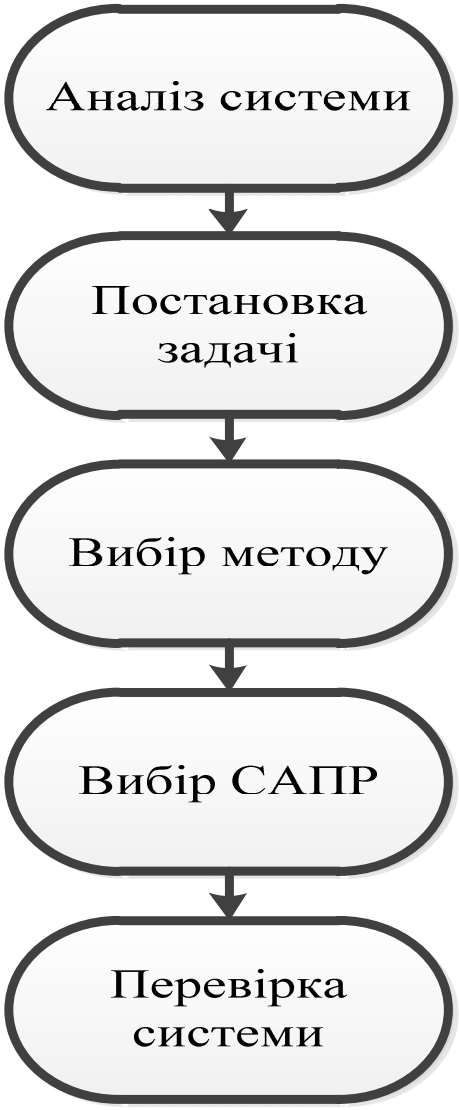


Рисунок 1.3 – Процес досягнення мети магістерської розробки

Для досягнення мети необхідно вирішити наступні задачі:

9) здійснити аналіз сучасних телемедичних систем;

10) провести дослідження основних модулів телемедицини;

11) проаналізувати сучасні алгоритми захисту інформації;

12) аргументувати вибір алгоритму захисту конфіденційної інформації в телемедицині;

13) вибрати шлях реалізації алгоритму, зокрема можливість застосування апарату нечіткої логіки;

14) розробити нечітку систему вибору алгоритму захисту інформації;
15) здійснити реалізацію розробленої системи;
16) провести симуляцію змодельованого засобу захисту.

2 РОЗРОБКА ПОЛІТИКИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В ТЕЛЕМЕДИЧНІЙ СИСТЕМІ

2.1 Дані в телемедичній системі, які потребують захисту

Основними групами користувачів телемедицини є лікуючий лікар, лікар-діагност, експерт, лаборант та адміністратор.

У базі даних зберігається інформація про користувачів системи, досліди пацієнтів, кількісні та якісні характеристики зображень, заключення експерта та ін. В процесі роботи із пацієнтами важливим елементом системи є логування дій користувачів. Уся інформація про дії лікарів, яка доступна для перегляду адміністратору системи, знаходиться у базі даних.

Для збереження конфіденційності даних пацієнтів уся інформація повинна шифруватися, щоб зловмисник не зміг ідентифікувати приналежність зображення з певним діагнозом до конкретного пацієнта.

Лікарю – діагносту чи експерту не потрібно вручну вибирати директорію із зображеннями для подальшого перегляду. Система автоматично при виборі пацієнта та досліду створює локальну копію файлів на стороні клієнта (лікаря – діагноста, експерта). Видалення локальної копії зображень умисно чи з необережності не призведе до втрати усіх файлів конкретного дослідження.

Тому варто комунікацію між усіма користувачами телемедичної системи здійснювати за допомогою віддаленої бази даних та віддаленого FTP–сервера. Хмарні технології — це парадигма, що передбачає віддалену обробку та зберігання даних.

Ця технологія надає користувачам мережі Інтернет, доступ до комп'ютерних ресурсів сервера і використання програмного забезпечення як онлайн-сервіса. Тобто якщо є підключення до Інтернету то можна виконувати

складні обчислення, опрацьовувати дані використовуючи потужності віддаленого сервера.

На FTP сервері варто також розташувати зображення, отримані під час проведення досліджень. Це спростить роботу самої системи, оскільки підвищить її продуктивність шляхом розвантаження оперативної та статичної пам’яті.

Файли, відібрані для досліду, лікуючим лікарем також автоматично завантажуються на FTPсервер, а відповідна директорія з ними шифрується. Даний підхід значно спрощує інтерфейс користувача та дозволяє зосередитись лікарям лише на опрацюванні зображень.

2.2 Алгоритми управління доступом до конфіденційної інформації телемедицини

Управління доступом – метод захисту інформації за рахунок регулювання використовування всіх інформаційних ресурсів, у тому числі автоматизованої інформаційної системи підприємства. Управління доступом включає наступні функції захисту:

1) ідентифікацію користувачів, персоналу і ресурсів інформаційної системи (привласнення кожному об'єкту персонального ідентифікатора);

2) аутентифікацію (встановлення автентичності) об'єкту або суб'єкта після пред'явленому їм ідентифікатору;

3) перевірку повноважень (перевірка відповідності дня тижня, часу доби, запрошуваних ресурсів і процедур встановленому регламенту);

4) дозвіл і створення умов роботи в межах встановленого регламенту;

5) реєстрацію (протоколювання) звернень до ресурсів, що захищаються;

6) реагування (сигналізація, відключення, затримка робіт, відмова в запиті) при спробах несанкціонованих дій.

Проте, застосування всіх відомих методів захисту даних інформаційної системи не гарантує збереження цілісності даних, тому розробка нових підходів залишається актуальною задачею.

Одним із шляхів розв’язку цього завдання є застосування нечіткої логіки до побудови системи захисту інформації та її апаратної реалізації.

Для здійснення захисту інформації в телемедицині необхідно визначити рівень доступу поточного клієнта до інформаційної системи. Крім того, варто враховувати ризик виникнення атаки через поточний канал передачі інформації, який може визначатися співвідношенням кількості звернень даного клієнта до кількості збоїв під час передачі даних через його канал.

На даний час відомі симетричні та асиметричні криптоалгоритми. Найпоширеніші серед них – симетричний DES, асиметричний RSA та на основі еліптичних кривих [5].

Інтенсивність інформаційних потоків постійно зростає, що призводить до росту актуальності задач захисту інформаційних ресурсів. Для забезпечення захисту електронних документів і створення захищеної автоматизованої системи в першу чергу використовують криптографічні методи захисту, що дозволяють забезпечити захист цілісності, авторства і конфіденційності електронної інформації і реалізувати їх у виді програмних чи апаратних засобів, що вмонтовуються в автоматизовану систему.

В умовах конкурентної боротьби збереження ведучих позицій і залучення нових клієнтів можливо лише за умови надання більшої кількості послуг і скорочення часу обслуговування.

Цього можна досягнути тільки за умови забезпечення необхідного рівня автоматизації всіх банківських операцій. У той же час, застосування обчислювальної техніки не тільки розв'язує виникаючі проблеми, але і приводить до появи нових, нетрадиційних для банку загроз, пов'язаних з можливістю випадкової чи навмисної модифікації і небезпекою несанкціонованого доступу до інформації особами, для яких вона не призначена.

У цих умовах на перший план виходять задачі захисту інформації й у тому числі впровадження криптографічних засобів. Однак аналіз існуючого становища показує, що рівень заходів щодо захисту інформації, як правило, відстає від темпів автоматизації. Таке відставання може обернутися надзвичайно серйозними наслідками.

Однією з основних причин цього відставання є нерозвиненість і нерегульованість ринку криптографічної продукції. При цьому недостатньо враховуються відмінності комерційної інформації від традиційних об'єктів криптографічного захисту (військові і державні секрети), що приводить до завищених вимог до засобів криптографічного захисту банківської інформації.

Вразливість інформації в автоматизованих комплексах обумовлюється великою концентрацією обчислювальних ресурсів, їхньою територіальною розподіленістю, довгостроковим збереженням великих обсягів даних на магнітних носіях, одночасним доступом до ресурсів великого числа користувачів різних категорій.

У цих умовах необхідність вживання заходів захисту, не викликає сумнівів. Однак тут існує ряд об'єктивних труднощів.

По-перше, виробники засобів захисту в основному пропонують окремі компоненти для рішення часткових задач, залишаючи вирішення питань формування системи захисту і сумісності цих засобів на кінцевих користувачів.

По-друге, для забезпечення надійного захисту необхідно вирішити цілий комплекс технічних і організаційних проблем і розробити відповідну документацію.

По-третє, неможливо в реальній складній системі передбачити і забезпечити захист від усіх дій кваліфікованого зловмисника. Необхідно постійно удосконалювати захист у процесі нагромадження нових знань.

Автоматизований комплекс можна вважати захищеним, якщо всі операції виконуються у відповідності із строго визначеними правилами, що забезпечують безпосередній захист об'єктів, ресурсів і операцій.

Основу для формування вимог до захисту складає список загроз. Коли такі вимоги відомі, можуть бути визначені відповідні правила забезпечення захисту. Ці правила, у свою чергу, визначають необхідні функції і засоби захисту. Чим більше вимог до захисту і відповідних правил, тим ефективніше механізми захисту і тим більше захищеним виявляється автоматизований комплекс.

В асиметричних системах необхідно застосовувати довгі ключі (512 бітів і більше). Довгий ключ різко збільшує час шифрування. Крім того, генерація ключів дуже тривала. Зате розподіляти ключі можна по незахищених каналах.

У симетричних алгоритмах використовують більш короткі ключі, тобто шифрування відбувається швидше. Але в таких системах складніша процедура розподілу ключів.

Тому при проектуванні захищеної системи часто застосовують і симетричні, і асиметричні алгоритми. Тому що система з відкритими ключами дозволяє розподіляти ключі й у симетричних системах, можна об'єднати в системі передачі захищеної інформації асиметричний і симетричний алгоритми шифрування. За допомогою першого розсилати ключі, другим - власне шифрувати передану інформацію .

Нижче наведено класифікацію сучасних алгоритмів шифрування.

- симетричні (із секретним, єдиним ключем, одноключові, single-key).
- потокові (шифрування потоку даних):
- з одноразовим чи нескінченним ключем (infinite-key cipher);
- з кінцевим ключем (система Вернама - Vernam);
- на основі генератора псевдовипадкових чисел (ПВЧ).
- блокові (шифрування даних поблочно):
- шифри перестановки (permutation, P-блоки);
- шифри заміни (підстановки, substitution, S-блоки):
- моноалфавітні (код Цезаря);
- поліалфавітні (шифр Віженера, циліндр Джефферсона, диск Уетстоуна, Enigma);

Складені:

- Lucipher (фірма IBM, США);
- DES (Data Encryption Standard, США);
- FEAL-1 (Fast Enciphering Algoritm, Японія);
- IDEA/IPES (International Data Encryption Algorithm/
- Improved Proposed Encryption Standard, фірма Ascom-Tech AG, Швейцарія);
- B-Crypt (фірма British Telecom, Великобританія);
- ГОСТ 28147-89 (СРСР); * Skipjack (США).
- Асиметричні (з відкритим ключем, public-key):
- Діффі-Хеллмана DH (Diffie, Hellman);
- Райвест-Шамір-Адлеман RSA (Rivest, Shamir, Adleman);
- Эль-Гамаль ElGamal.

DES (англ. Data Encryption Standard) — це симетричний алгоритм шифрування певних даних , стандарт шифрування прийнятий урядом США із 1976 до кінця 1990-х, з часом набув міжнародного застосування. Ще з часу свого розроблення алгоритм викликав неоднозначні відгуки. Оскільки DES містив засекречені елементи своєї структури, породжувались побоювання щодо можливості контролю з боку Національного Агентства Безпеки США (англ. National Security Agency).

Алгоритм піддавався критиці за малу довжину ключа, що, врешті, після бурхливих обговорень та контролю академічної громадськості, не завадило йому стати загальноприйнятим стандартом. DES дав поштовх сучасним уявленням про блочні алгоритми шифрування та криптоаналіз.

DES є блочним шифром - дані шифруються блоками по 64 біти - 64 бітний блок явного тексту подається на вхід алгоритму, а 64-бітний блок шифрограми отримується в результаті роботи алгоритму. Крім того, як під час шифрування, так і під час дешифрування використовується один і той самий алгоритм (за винятком дещо іншого шляху утворення робочих ключів).

Ключ має довжину 56 біт (як правило, в джерельному вигляді ключ має довжину 64 біти, де кожний 8-й біт є бітом паритету, крім того, ці контрольні біти можуть бути винесені в останній байт ключа). Ключем може бути довільна 64-бітна комбінація, яка може бути змінена у будь-який момент часу. Частина цих комбінацій вважається слабкими ключами, оскільки може бути легко визначена. Безпечність алгоритму базується на безпечності ключа.

На найнижчому рівні алгоритм є ніщо інше, ніж поєднання двох базовних технік шифрування: перемішування і підстановки. Цикл алгоритму, з яких і складається DES є комбінацією цих технік, коли як об'єкти перемішування виступають біти тексту, ключа і блоків підстановок.

Ідея застосування методів криптографії з відкритим ключем полягає в наступному.

Перший ключ використовується для шифрування – він вільно розповсюджується. Розшифрувати зашифроване повідомлення можна використовуючи таємний ключ. Дешифрування криптотексту, без відомостей про закритий ключ практично неможливе. Вирішення задачі обчислення закритого ключа по відомому відкритому практично є не можливим [2-6].

Основна перевага криптографії з відкритим ключем – спрощений механізм обміну ключами. При здійсненні комунікації по відкритому каналу зв’язку передається тільки відкритий ключ і при цьому, зникає необхідність у наявності спеціального захищеного каналу зв’язку для передачі ключа розшифрування інформації.

Механізм обміну ключами можна в деякій мірі модифікувати, ввівши у систему деяку третю сторону, на яку покладено функцію генерування і розподілення ключів між учасниками системи інформаційного обміну, як наведено на рисунку 2.1, а також третя сторона має гарантувати надійність виконання даних процедур [7].

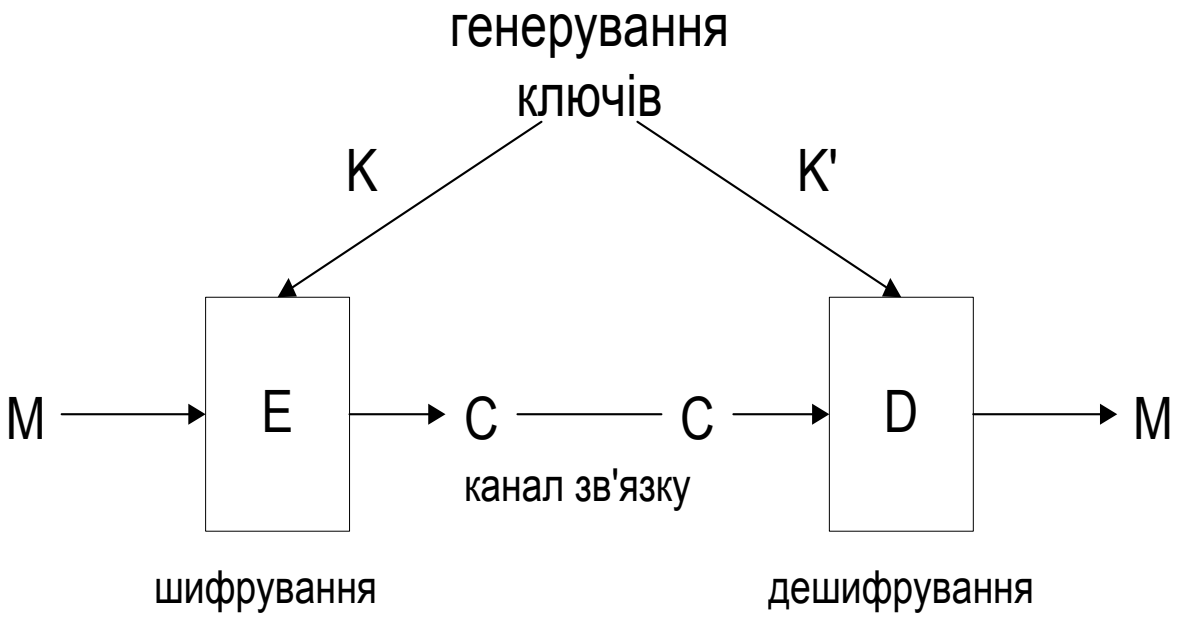


Рисунок 2.1 – Асиметрична криптосхема з третьою стороною

Треба зазначити, що з появою систем з відкритим ключем поняття про захист інформації, а разом з тим і криптографії значно розширилися. Якщо раніше основною задачею криптографічних систем було надійне зашифрування інформації, то на даний час область застосування криптографії включає також цифровий підпис (аутентифікацію), ліцензування, нотаризацію (свідчення), розподілене керування, електронні гроші, схеми голосування та ін. [1, 5].

Наведемо ряд сучасних асиметричних схем та обчислювальні проблеми, на яких базується їхня стійкість:

- RSA – факторизація (розбиття на прості співмножники) цілих чисел;
- Rabin – факторизація цілих чисел та знаходження квадратного кореня великого цілого числа;
- ElGamal – задача обчислення дискретного логарифму;
- McElice – декодування лінійного коду;
- Merkle-Hellman та Chor-Rivest скриньки – задача підмножини сум;
- Golgwasser-Micali та Blub- Golgwasser - теорія імовірності квадратних рівнянь.

Через особливості алгоритмів, що лежать в основі систем з відкритим ключем, їх швидкодія при обробці одиничних блоків інформації зазвичай в десятки разів менше, чим швидкодія симетричних криптосистем із блоком такої ж довжини [2], як і їхня програмна, так і апаратні реалізації.

Обчислення ключів здійснюється одержувачем повідомлень або ж адміністратором, який виконує функцію надання користувачам ключів. Отримувачу залишається таємний ключ, той, що буде потім використовуватися для розшифрування. Відкритий ключ вільно розповсюджується по мережі потенційним відправникам повідомлень.

Користаючись цим відкритим ключем, будь-який абонент мережі може зашифрувати повідомлення і послати його особі, що має секретний ключ. Особливо важливо те, що функції шифрування і дешифрування оборотні лише тоді, коли вони забезпечуються строго взаємозалежною парою ключів, а відкритий ключ повинний являти собою необоротну функцію від секретного ключа. Подібним чином шифротекст повинний являти собою необоротну функцію відкритого тексту, що в корені відрізняється від симетричного шифрування.

Найпопулярнішою криптосистемою з відкритим ключем є запропонована 1977 року система RSA. RSA (абревіатура від прізвищ Rivest, Shamir та Adleman) — криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності задачі факторизації великих цілих чисел.

RSA став першим алгоритмом такого типу, придатним і для шифрування, і для цифрового підпису. Алгоритм застосовується до великої кількості криптографічних застосунків.

Алгоритм RSA складається з 4 етапів: генерації ключів, шифрування, розшифрування та розповсюдження ключів.

Безпека алгоритму RSA побудована на принципі складності факторизації цілих чисел. Алгоритм використовує два ключі — відкритий (public) і секретний (private), разом відкритий і відповідний йому секретний ключі утворюють пари

ключів (keypair). Відкритий ключ не потрібно зберігати в таємниці, він використовується для шифрування даних. Якщо повідомлення було зашифровано відкритим ключем, то розшифрувати його можна тільки відповідним секретним ключем.

Еліптична криптографія — розділ криптографії, який вивчає асиметричні криптосистеми, засновані на еліптичних кривих над кінцевими полями. Головна перевага еліптичної криптографії полягає в тому, що на сьогодні є невідомим існування субекспоненціальних алгоритмів вирішення завдань дискретного логарифмування. Використання еліптичних кривих для створення криптосистем було незалежно запропоновано Нілом Коблицем[en] та Віктором Міллером[en] у 1985 році.[1]

Асиметрична криптографія заснована на складності рішення деяких математичних задач. Ранні криптосистеми з відкритим ключем, такі як алгоритм RSA, криптостійкі завдяки тому, що складно розкласти велике число на прості множники. При використанні алгоритмів на еліптичних кривих припускається, що не існує субекспоненційних алгоритмів для вирішення завдання дискретного логарифмування в групах їх точок. При цьому порядок групи точок еліптичної кривої визначає складність завдання. Вважається, що для досягнення такого ж рівня криптостійкості як і в RSA, потрібні групи менших порядків, що зменшує витрати на зберігання та передачу інформації. Наприклад, на конференції RSA 2005 Агентство національної безпеки оголосила про створення «Suite B», у якому використовуються виключно алгоритми еліптичної криптографії, причому для захисту інформації класифікованої до «Top Secret» використовуються всього лише 384-бітові ключі.

Як у випадку із наведеною вище криптосистемою, еліптичні криві (ЕК) також використовують обчислювальну складність знаходження дискретного логарифма в множині (кільці) цілих чисел за простим модулем. У загальному випадку еліптичну криву можна задати формулою (2.1), зовнішній вигляд якої наведено на рисунку 2.2 [5].

$$y^2 = x^3 + ax + b \tag{2.1}$$

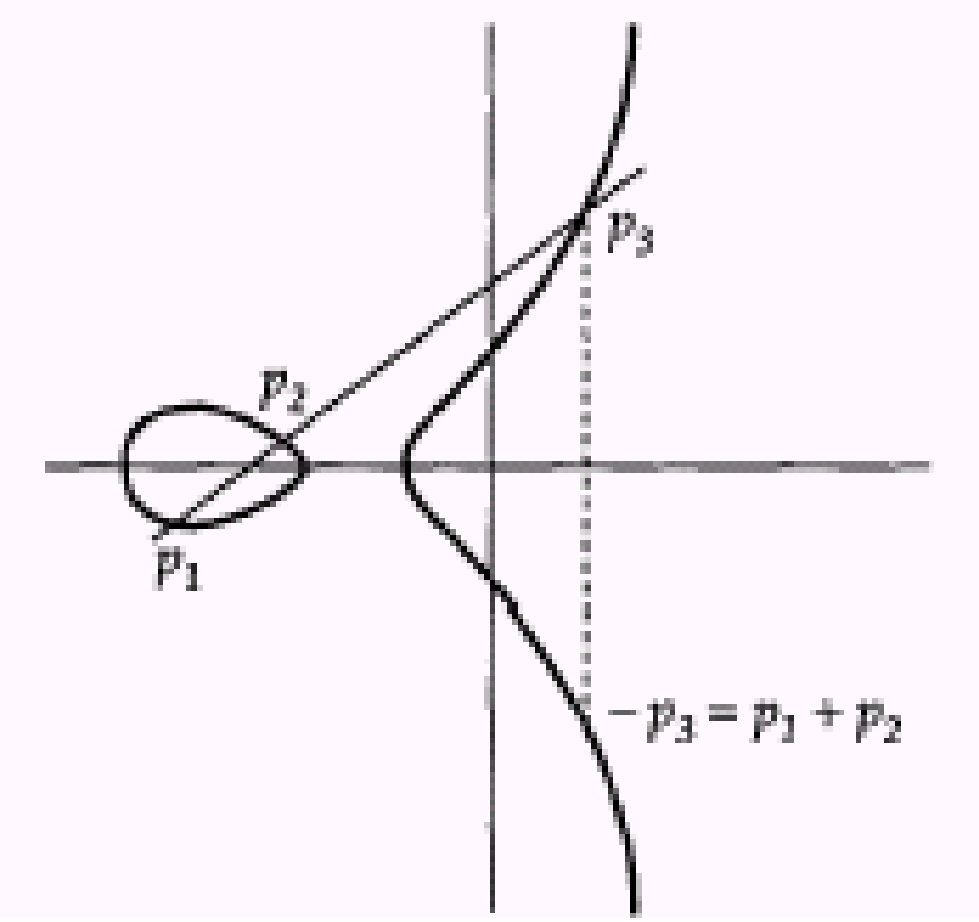


Рисунок 2.2 – Еліптична крива

Розглянемо принципи побудови і використання еліптичних кривих в криптографії.

Кубічна крива на площині XY, задана рівнянням $y^2 = x^3 + ax + b$, що не має особливих точок, називається еліптичною кривою [3]. В реальних криптосистемах використовується рівняння

$$y^2 = x^3 + ax + b \pmod{p}, \tag{2.2}$$

де a, b належать полю GF(p), $4a^3 + 27b^2 \pmod p \neq 0$, p – просте число.

Множина $E_p(a, b)$ містить всі точки (x, y), $x \geq 0$, $p > y$, що задовольняють рівняння (2.2), і точку в нескінченності O, яка є нулем для площини еліптичних кривих. Кількість точок еліптичної кривої позначається $\#E_p(a, b)$.

Множина точок $E_p(a, b)$ має такі властивості:

– якщо $P = (x, y)$ є точкою ЕК, то $(x, y) + (x, -y) = O$; точка $(x, -y)$ позначається як $–P$;

– якщо $P=(x_1, y_1)$ і $Q = (x_2, y_2)$, де $P \neq Q$, то $P + Q = (x_3, y_3)$ обчислюється так:

$$x_3 = (y_2–y_1)/(x_2–x_1)–x_1–x_2;$$
$$y_3 = –y_1–(y_2–y_1)(x_2–x_1)/(x_2–x_1) \quad (2.3)$$

– якщо $P = Q$, то подвоєння точки [2] $P = (x_3, y_3)$ обчислюється за формулою:

$$x_3 = ((3x_1^2+a)/2/y_1)^2–2x_1;$$
$$y_3 = –y_1–(3x_1^2+a)/2/y_1 \quad (2.4)$$

Одним із криптографічних застосувань еліптичних кривих є розподіл ключів. Криптографічний протокол обміну ключами з використанням еліптичної кривої виглядає таким чином:

– користувачі повинні обирати і повідомити всім форму еліптичної кривої та цілу точку G на цій кривій, яка є генеруючою точкою;

– користувач I повинен обрати ціле число k і знайти точку $P_A = k*G$ (додати точку G до самої себе k разів);

– користувач II повинен обрати число m і обчислити точку $P_B=m*G$. Після цього вони обмінюються своїми результатами і їх спільним секретним ключем стає точка $k*m*G$.

Для розкриття такого протоколу потрібно за відомими $k*G$ і G обчислити $k<p$, що є аналогом важкої задачі дискретного логарифмування у випадку алгоритму RSA: легко обчислити P за відомими k і G, проте важко обчислити k за відомими P і G.

Однією з проблем криптографічного застосування еліптичних кривих є вибір надійної випадкової кривої. Вирішення цієї проблеми визначає стійкість результуючої криптосистеми.

2.3 Застосування нечіткої логіки в задачах захисту інформації

У [3] автори запропонували нечіткі системи прийняття рішень для діагностики раку молочної залози. Рак молочної залози є найбільш далекоглядним захворюванням сьогодні, тому первинне виявлення раку молочної залози є дуже значним. Запропонований документ був забезпечений штучними інтелектуальними методами, такими як нечітка логіка для правильного прийняття рішень. На основі нечітких правил використовуються експертні знання для вирішення симптомів пацієнта та точного рішення відповідно до побудованих правил [3].

Авторами [4] підсумовуються суттєві відмінності в системах нечітких висновків типу Маддані та типу Сугено для діагностики цукрового діабету. Для їх реалізації розробники використали MATLAB Fuzzy Toolbox.

Нечіткі системи, керовані правилами, підходять для медичної області, де інтерпретативність є основною проблемою. Медичний домен є надзвичайно важливим для даних та використовує дані електронних медичних записів для

побудови бази знань, а нечіткі набори є критичними. Багатокористувацькі змінні часто необхідні для визначення правильного та персоналізованого діагнозу, що зазвичай ускладнює отримання точних та своєчасних рішень.

У [5] запропоновано та впроваджено нову семантично інтерпретовану структуру бази знань для діагностики діабету. В даній системі використовуються численні аспекти нечіткого висновку про знання, міркування онтології та нечіткий аналітичний процес ієрархії для забезпечення більш інтуїтивно зрозумілого та точного дизайну.

Запропонована система пропонує безліч унікальних і критичних удосконалень у відношенні реалізації точної, динамічної, семантично інтелектуальної та інтерпретованої бази знань. Розроблена система розглядає семантичну схожість онтології з ускладненнями та симптомами діабету в процесі оцінки нечітких правил, була протестована, використовуючи реальний набір даних, і результати показують, як запропонована система допомагає лікарям та пацієнтам точно діагностувати цукровий діабет.

Вдосконалення нечіткої системи як, наприклад, у [7], дозволяє будувати ефективні діагностичні моделі, які можна успішно застосовувати у сучасній телемедицині.

З аналізу сучасних публікацій в сфері телемедицини можна зробити висновок, що застосування апарату нечіткої логіки дозволяє розробляти швидкі та високопродуктивні системи діагностування патологічних станів пацієнтів.

Теорія нечіткої логіки є узагальненням класичної формальної логіки. Дане поняття було вперше запропоноване американським ученим Лотфі Заде в 1965 р. Основною причиною появи нової теорії стала наявність нечітких і наближених міркувань при описі людиною процесів, систем та об'єктів [3].

Побудова нечіткої системи на основі нечіткої логіки є актуальною задачею, оскільки дозволяє здійснювати захист інформації без глибоких спеціальних знань у цій галузі.

Характеристикою нечіткої множини виступає функція приналежності. Для опису нечітких множин вводяться поняття нечіткої і лінгвістичної змінних. Нечітка змінна описується набором (*N*,*X*,*A*), де *N* – це назва змінної, *X* – універсальна множина (область міркувань), *A* – нечітка множина на *X*. Значеннями лінгвістичної змінної можуть бути нечіткі змінні, тобто лінгвістична змінна знаходиться на більш високому рівні, ніж нечітка змінна. Кожна лінгвістична змінна складається з:

- назви;
- множини своїх значень, яка також називається базовою терм-множиною *T*. Елементами базової терм-множини є назви нечітких змінних;
- універсальної множини *X*;
- синтаксичного правила *G*, по якому генеруються нові терми із застосуванням слів природної або формальної мови;
- семантичного правила *P*, яке кожному значенню лінгвістичної змінної ставить у відповідність нечітку підмножину множини *X*.

Існує понад десяток типових форм кривих для задання функцій приналежності. Найбільшого поширення набули: трикутна, трапецеїдальна і Гауссова функції приналежності [3].

Трикутна функція приналежності визначається трійкою чисел (*a*,*b*,*c*) і її значення в точці *x* обчислюється згідно виразу:

$$MF(x)=\begin{cases}1-\dfrac{b-x}{b-a}, a\le x\le b\\ 1-\dfrac{x-c}{c-b}, b\le x\le c\\ 0, \text{в інших випадках}\end{cases} \qquad (2.5)$$

При (*b*-*a*)=(*c*-*b*) маємо випадок симетричної трикутної функції приналежності, яка може бути однозначно задана двома параметрами з трійки (*a*,*b*,*c*).

Аналогічно для задання трапецеїдальної функції приналежності необхідна четвірка чисел (*a*,*b*,*c*,*d*):

$$MF(x)=\begin{cases}1-\dfrac{b-x}{b-a}, a\le x\le b\\ 1, b\le x\le c\\ 1-\dfrac{x-c}{d-c}, c\le x\le d\\ 0, \text{в інших випадках}\end{cases} \tag{2.6}$$

При (*b*-*a*)=(*d*-*c*) трапецеїдальна функція приналежності набирає симетричного вигляду.

Функція приналежності гауссового типу описується формулою

$$MF(x)=exp\left[-\left(\frac{x-c}{\sigma}\right)^2\right] \tag{2.7}$$

і оперує двома параметрами. Параметр *c* позначає центр нечіткої множини, а параметр σ відповідає за крутизну функції.

Основою для проведення операції нечіткого логічного висновку є база правил, що містить нечіткі висловлення у формі "Якщо-то" і функції приналежності для відповідних лінгвістичних термів. При цьому повинні дотримуватися наступні умови:

1) існує хоча б одне правило для кожного лінгвістичного терма вихідної змінної;

2) для будь-якого терма вхідної змінної є хоч би одне правило, в якому цей терм використовується як передумова (ліва частина правила).

У загальному випадку механізм логічного висновку включає чотири етапи: введення нечіткості (фазифікація), нечіткий висновок, композиція і приведення до чіткості, або дефазифікація.

Алгоритми нечіткого висновку розрізняються головним чином видом використовуваних правил, логічних операцій і різновидом методу дефазифікації. Розроблені моделі нечіткого висновку Мамдані, Сугено, Ларсена, Цукамото.

Механізм Мамдані − це найбільш поширений спосіб логічного висновку в нечітких системах. В ньому використовується мінімаксна композиція нечітких множин. Даний механізм включає наступну послідовність дій:

1) процедура фазифікації: визначаються степені істинності, тобто значення функцій приналежності для лівих частин кожного правила (передумов);

2) нечіткий висновок;

3) композиція або об'єднання отриманих усічених функцій, для чого використовується максимальна композиція нечітких множин;

4) дефазифікація або приведення до чіткості. Існує декілька методів дефазифікації. Наприклад, метод середнього центру або центроїдний метод.

Класичні нечіткі системи володіють тим недоліком, що для формулювання правил і функцій приналежності необхідно залучати експертів тієї або іншої наочної області, що не завжди удається забезпечити.

Адаптивні нечіткі системи вирішують цю проблему. У таких системах підбір параметрів нечіткої системи проводиться в процесі навчання на експериментальних даних.

Алгоритми навчання адаптивних нечітких систем відносно трудомісткі і складні в порівнянні з алгоритмами навчання нейронних мереж, і, як правило, складаються з двох стадій: генерації лінгвістичних правил; коректування функцій приналежності.

Перше завдання відноситься до задання перераховного типу, друга – до оптимізації в безперервних просторах. При цьому виникає певне протиріччя: для генерації нечітких правил необхідні функції приналежності, а для проведення нечіткого висновку – правила. Крім того, при автоматичній генерації нечітких правил необхідно забезпечити їх повноту і непротирічність [3].

Simulink – інтерактивний інструмент для моделювання, імітації та аналізу динамічних систем. Він дає можливість будувати графічні блок-діаграми, імітувати динамічні системи, досліджувати працездатність системи і вдосконалювати проекти.

Simulink повністю інтегрований з MATLAB, забезпечуючи негайний доступ до широкого спектру інструментів аналізу та проектування. Simulink також інтегрується з Stateflow для моделювання поведінки системи та певні події. Ці переваги роблять Simulink найпопулярнішим інструментом для проектування систем управління та комунікації, цифрової обробки та інших додатків моделювання.

При моделюванні за допомогою Simulink реалізується принцип візуального програмування, у відповідності до якого користувач на екрані із бібліотеки стандартних блоків створює модель пристрою і здійснює розрахунки.

При цьому, в залежності від класичних методів моделювання, користувачу не потрібно досконало вивчати мову програмування та численні методи математики, достатньо загальних знань, які необхідні при роботі на комп'ютері, і, звичайно, знань предметної області, в якій він працює.

Simulink є достатньо самостійним інструментом MATLAB, і при роботі з ним зовсім не потрібно знати сам MATLAB і решта його додатків. З іншого боку, доступ до функцій MATLAB та інших його інструментів залишається відкритим і їх можна використовувати в Simulink.

Частина пакетів, які входять в його склад, вбудовані в Simulink (наприклад, LTI-Viewer додатку

Control System Toolbox – пакета для розробки систем керування). Є також додаткові бібліотеки блоків для різних областей застосування (наприклад, Power System Blockset – моделювання електротехнічних засобів, Digital Signal Processing Blockset – набір блоків для розробки цифрових пристроїв і т.д.).

При роботі з Simulink користувач має можливість модернізувати бібліотечні блоки, створювати свої власні, а також складати нові бібліотеки блоків.

Крім того, при моделюванні користувач може вибрати метод вирішення диференційних рівнянь, а також спосіб зміни модельного часу (з фіксованим чи змінним кроком).

Під час моделювання є можливість слідкувати за процесами, які відбуваються в системі. Для цього використовуються спеціальні пристрої спостереження, які входять в склад бібліотеки Simulink.

Результати моделювання можуть бути представлені у вигляді графіків чи таблиць.

Перевага Simulink полягає також в тому, що він дозволяє доповнювати бібліотеки блоків за допомогою підпрограм, написаних як на мові MATLAB, так і на мовах C + +, Fortran і Ada.

Система MATLAB/Simulink містить вбудований генератор коду мови опису апаратних засобів HDL (Simulink HDL Coder) і орієнтований на підтримку стимулятора VHDL ModelSim. Simulink HDL Coder — програмний продукт для генерації

VHDL-коду без прив’язки до конкретної архітектури ПЛІС та платформи по Simulink-моделях та граф-автоматах (Stateflow-діаграми). Система MATLAB/Simulink ефективна також при проектуванні цифрових фільтрів для реалізації в базисі ПЛІС і процесорів, оскільки містить Filter Design HDL Coder.

3 НЕЧІТКА СИСТЕМА ВИБОРУ АЛГОРИТМУ ШИФРУВАННЯ

3.1 Загальна схема нечіткої системи

Багато науковців застосовують методи штучного інтелекту для розробки нових систем діагностування, зокрема апарат нечіткої логіки.

Використовуючи комунікаційні технології, покращуються методи швидкого і кращого діагностування та методів надання медичної допомоги. Швидкі зв'язки між лікарями та пацієнтами здійснюються завдяки вдосконаленню телемедичних технологій.

Наприклад, у дослідженні [2] розроблено новий метод діагностики травмованої селезінки за наявності розриву, контузії, активної кровотечі або гематоми через травму черевної порожнини, використовуючи телемедицину на основі таблеток. Клініцисти повідомляли електронною поштою та діагностували патологічні результати, які належать 10 пацієнтам. Завдяки більш швидкій діагностиці запропонована авторами система зменшує смертність і захворюваність невідкладних пацієнтів.

У [3] автори запропонували нечіткі системи прийняття рішень для діагностики раку молочної залози. Рак молочної залози є найбільш далекоглядним захворюванням сьогодні, тому первинне виявлення раку молочної залози є дуже значним.

Запропонований документ був забезпечений штучними інтелектуальними методами, такими як нечітка логіка для правильного прийняття рішень. На основі нечітких правил використовуються експертні знання для вирішення симптомів пацієнта та точного рішення відповідно до побудованих правил [3].

Авторами [4] підсумовуються суттєві відмінності в системах нечітких висновків типу Маддані та типу Сугено для діагностики цукрового діабету. Для їх реалізації розробники використали MATLAB Fuzzy Toolbox. Нечіткі системи,

керовані правилами, підходять для медичної області, де інтерпретативність є основною проблемою.

Медичний домен є надзвичайно важливим для даних та використовує дані електронних медичних записів для побудови бази знань, а нечіткі набори є критичними. Багатокористувацькі змінні часто необхідні для визначення правильного та персоналізованого діагнозу, що зазвичай ускладнює отримання точних та своєчасних рішень.

У [5] запропоновано та впроваджено нову семантично інтерпретовану структуру бази знань для діагностики діабету. В даній системі використовуються численні аспекти нечіткого висновку про знання, міркування онтології та нечіткий аналітичний процес ієрархії для забезпечення більш інтуїтивно зрозумілого та точного дизайну.

Запропонована система пропонує безліч унікальних і критичних удосконалень у відношенні реалізації точної, динамічної, семантично інтелектуальної та інтерпретованої бази знань. Розроблена система розглядає семантичну схожість онтології з ускладненнями та симптомами діабету в процесі оцінки нечітких правил, була протестована, використовуючи реальний набір даних, і результати показують, як запропонована система допомагає лікарям та пацієнтам точно діагностувати цукровий діабет.

Вдосконалення нечіткої системи як, наприклад, у [7], дозволяє будувати ефективні діагностичні моделі, які можна успішно застосовувати у сучасній телемедицині.

З аналізу сучасних публікацій в сфері телемедицини можна зробити висновок, що застосування апарату нечіткої логіки дозволяє розробляти швидкі та високопродуктивні системи діагностування патологічних станів пацієнтів.

З метою вибору алгоритму шифрування (DES, RSA чи на основі еліптичних кривих) для кожного окремого клієнта телемедицини варто використати нечітку логіку.

В загальному схема вибору алгоритму захисту інформації зображена на

рисунку 3.1.

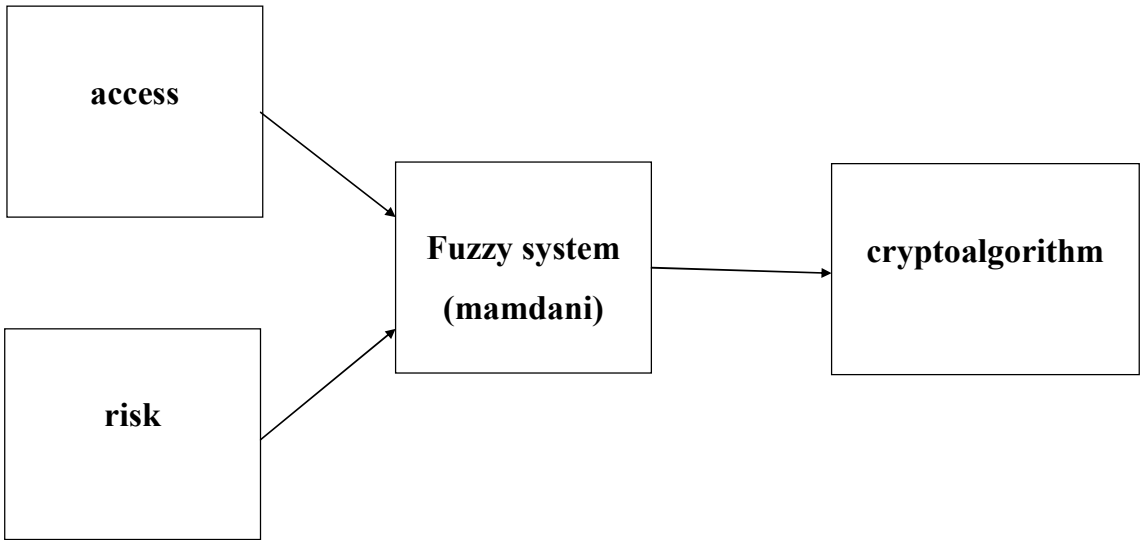


Рисунок 3.1 – Загальна схема розробленої нечіткої системи

В даному випадку в якості критеріїв вибору виступають рівень доступу клієнта до інформації (access) та ризик виникнення атаки при передачі інформації поточному клієнту (risk), а підсистемою вибору є система обробки нечіткої інформації на основі механізму Мамдані. Виходом такої системи є один з криптоалгоритмів, відповідний вхідним критеріям вибору і застосовуючи який комп'ютерна система забезпечить свою оптимальну роботу.

В інженерних задачах застосовується, як правило, механізм нечіткого висновку Мамдані [6, 7]. В ньому використовується мінімаксна композиція нечітких множин. Даний механізм включає наступну послідовність дій [8]:

1) процедура фазифікації: визначаються степені істинності, тобто значення функцій належності для лівих частин кожного *i*-го правила (передумов);

2) нечіткий висновок. Спочатку визначаються мінімальний рівень "відсічення" для лівої частини кожного з правил, а потім знаходяться "усічені" функції належності висновку;

3) композиція або об'єднання отриманих "усічених" функцій, для чого використовується максимальна композиція нечітких множин;

4) дефазифікація або приведення до чіткості. Існує декілька методів дефазифікації. Наприклад, метод середнього центру або центроїдний метод. Геометричний зміст такого значення – центр ваги для кривої функції належності отриманого виходу.

Схематично механізм Мамдані має вигляд, поданий на рисунку 3.2.

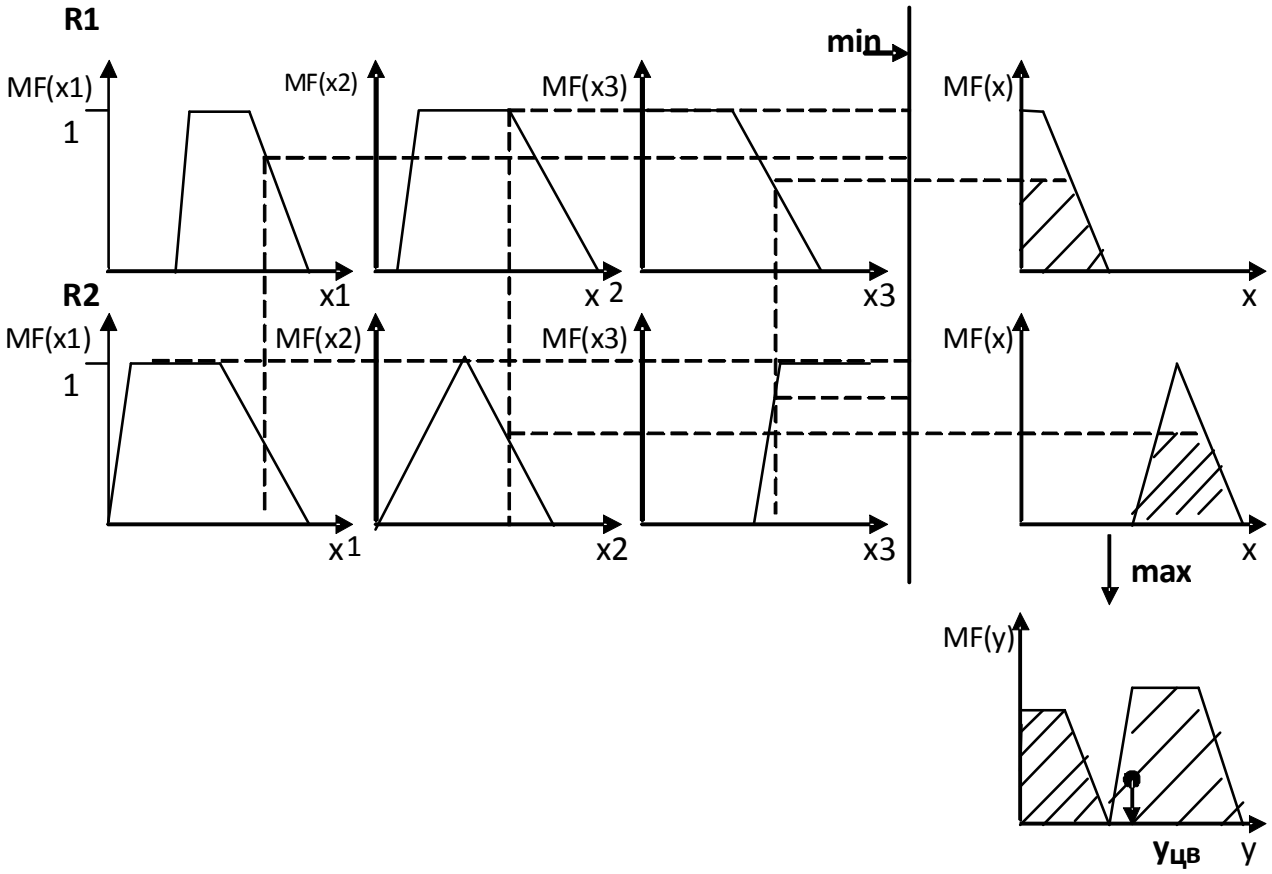


Рисунок 3.2 – Механізм Мамдані

3.2 Реалізація нечіткої системи вибору алгоритму шифрування

Застосовуючи засіб Fuzzy Logic Toolbox середовища MATLAB 7.7.0 (R2008b), можна побудувати запропоновану нечітку систему вибору криптоалгоритму.

Загальна схема розробленоъ нечыткоъ системи подана на рисунку 3.3.

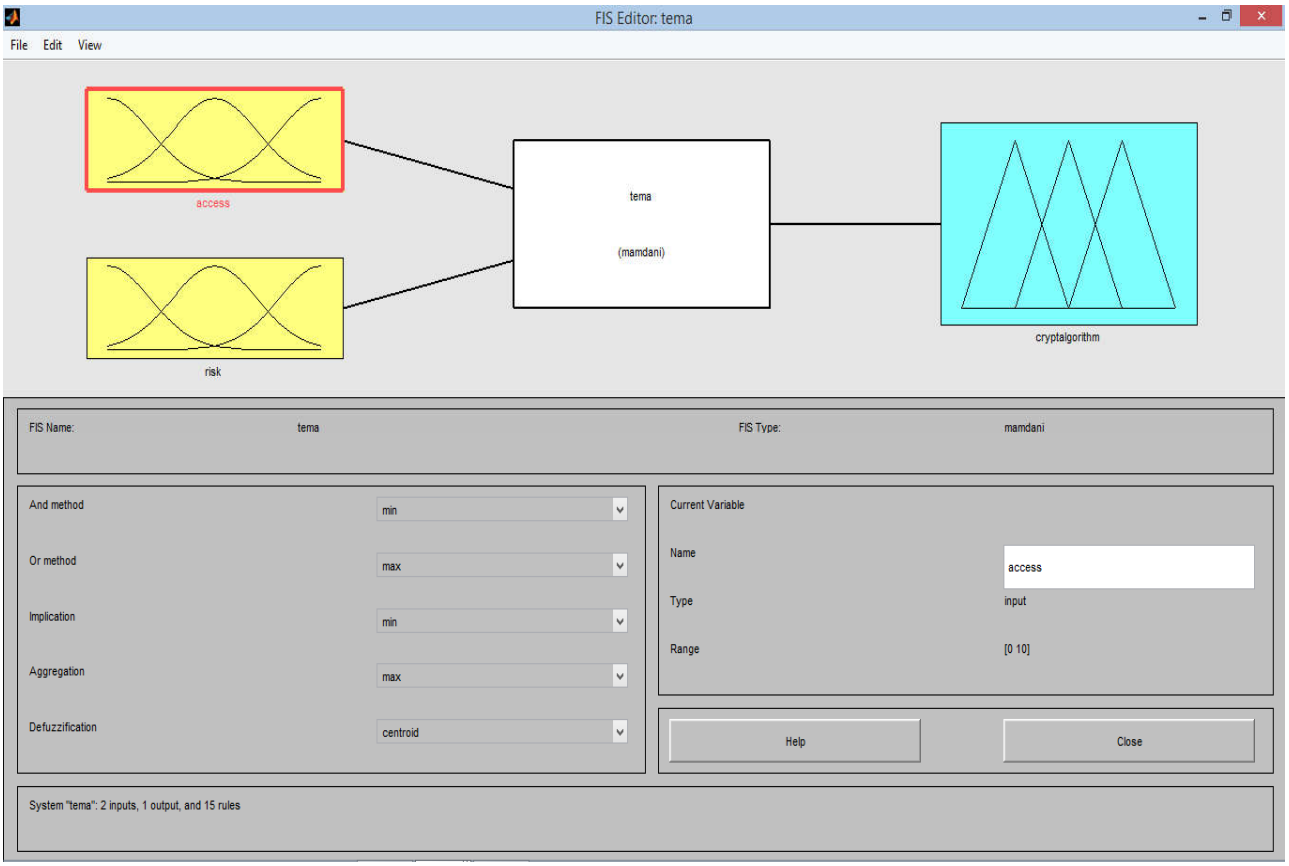


Рисунок 3.3 – Розроблена нечітка система в середовищі MATLAB

Значення функцій належності вхідних змінних *access* та *risk* задається трапецевидною функцією, що визначається четвіркою чисел (*a*,*b*,*c*,*d*), які позначають абсциси вершин трапеції.

Функція належності виходу *cryptoalgorithm* задається трикутною формою, яка залежить від трьох змінних (*a*,*b*,*c*) (абсциси вершин трикутника) [9] при чому

в даному випадку має місце випадок симетричної трикутної функції належності, тобто (*b*-*a*)=(*c*-*b*).

Функції належності для змінних *access* та *risk*, подані на рисунках 3.4 та 3.5, відповідно. Вони поділені на три інтервали кожна для точного опису змінних, зокрема, для опису рівня доступу до інформації застосовується змінна *low*, що позначає низький рівень доступу (може надаватися, наприклад, новим клієнтам), *middle* - середній рівень та *high* - високий рівень доступу (може надаватися адміністратору інформаційної системи).

Для задання рівня ризику виникнення атаки пропонуються змінні *low*, *middle* та *high*, що відповідають низькому, середньому та високому рівню.

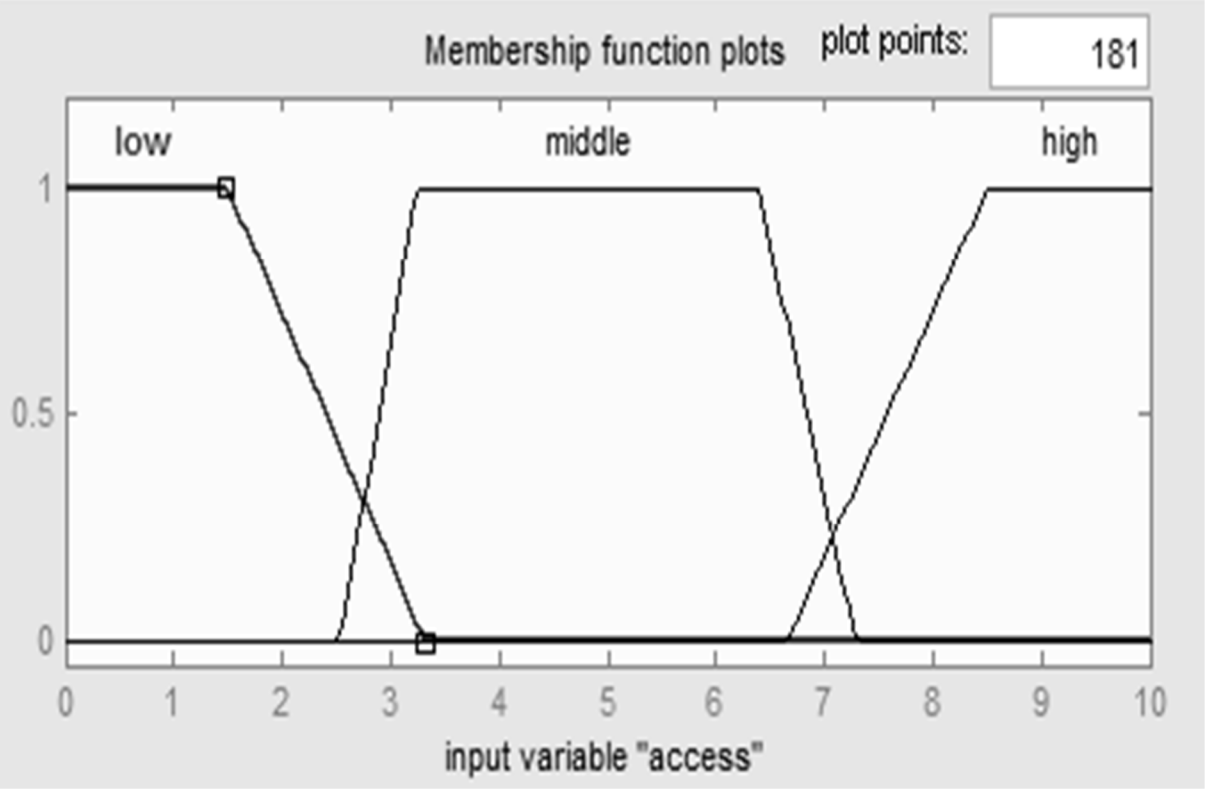


Рисунок 3.4 - Функції належності змінної *access*

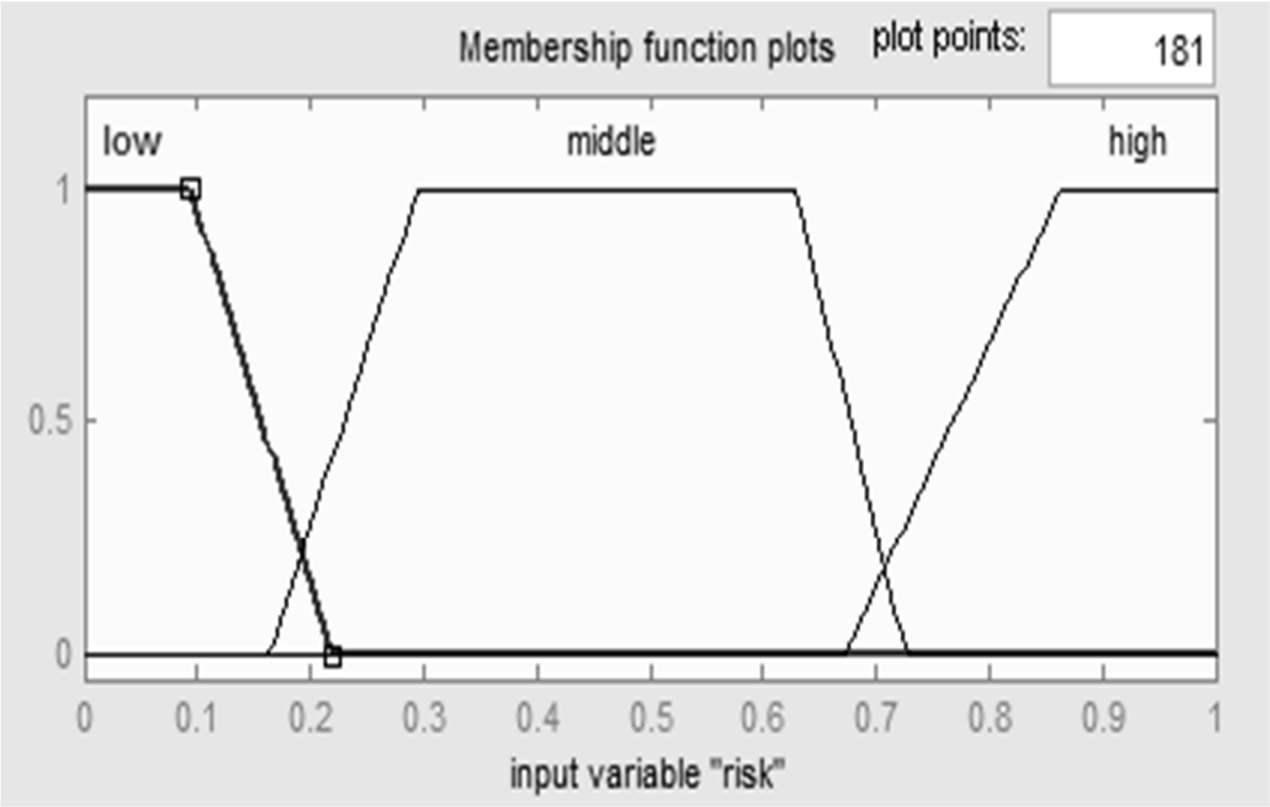


Рисунок 3.5 - Функції належності змінної *risk*.

Функції належності для вихідної змінної *cryptoalgorithm* зображено на рисунку 3.6.

Вони позначаються однаковими інтервалами на осі ординат для точного визначення центру ваги, що позначає нечіткий висновок системи. *None* позначає відсутність необхідності застосування алгоритму захисту інформації (наприклад, у випадку, коли до інформаційної системи звертається адміністратор), *DES*, *RSA* та *EC* – криптоалгоритм DES, RSA та на основі еліптичних кривих, відповідно. Кожен з цих алгоритмів має свої переваги і недоліки, свій рівень стійкості та продуктивності, які описані в [5].

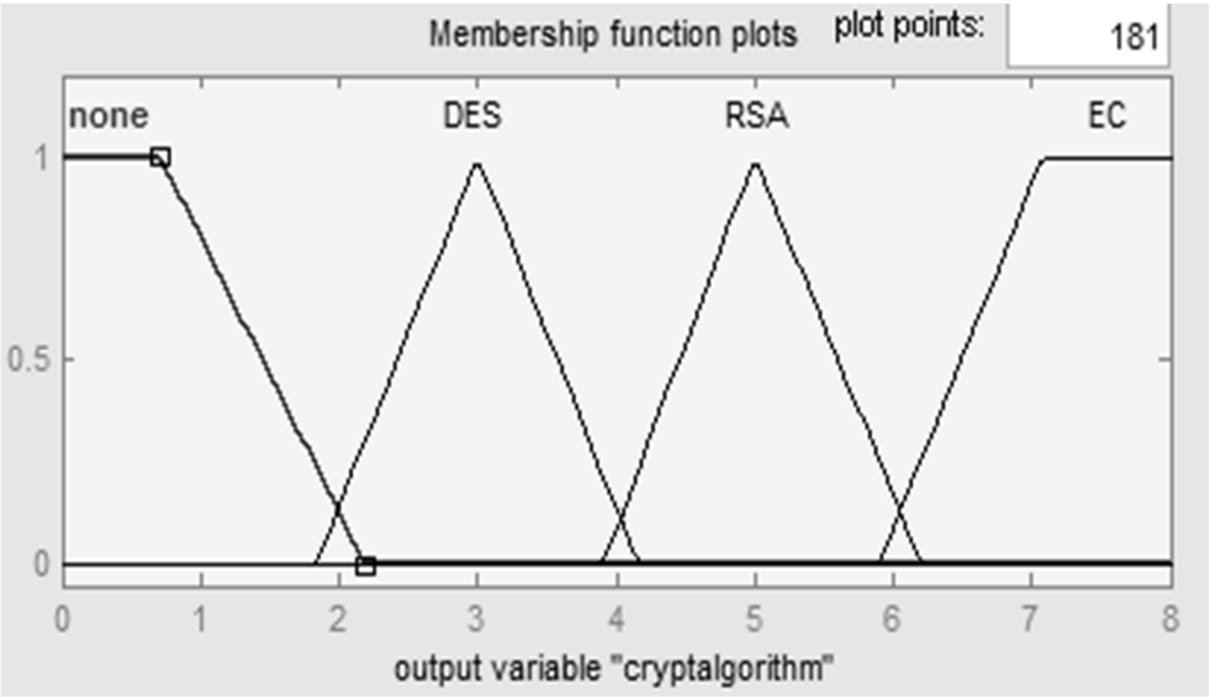


Рисунок 3.6 - Функції належності змінної *method*

База знань для побудови даної нечіткої моделі складається з правил типу «якщо - то» [9], усі вхідні змінні мають по три нечітких стани і ще один стан, коли значення вхідної змінної не задане системою. Випадок, коли значення усіх вхідних змінних не задані, на практиці неможливий, тому кількість правил нечіткого висновку досліджуваної системи $N = 4 \cdot 4 - 1 = 15$.

3.3 Верифікація та тестування запропонованої нечіткої системи

Для здійснення процесу тестування та верифікації варто використати засіб RuleViewer, який входить до Matlab Fuzzy Toolbox.

База правил розробленої нечіткої системи має вигляд, зображений на рисунку 3.7.

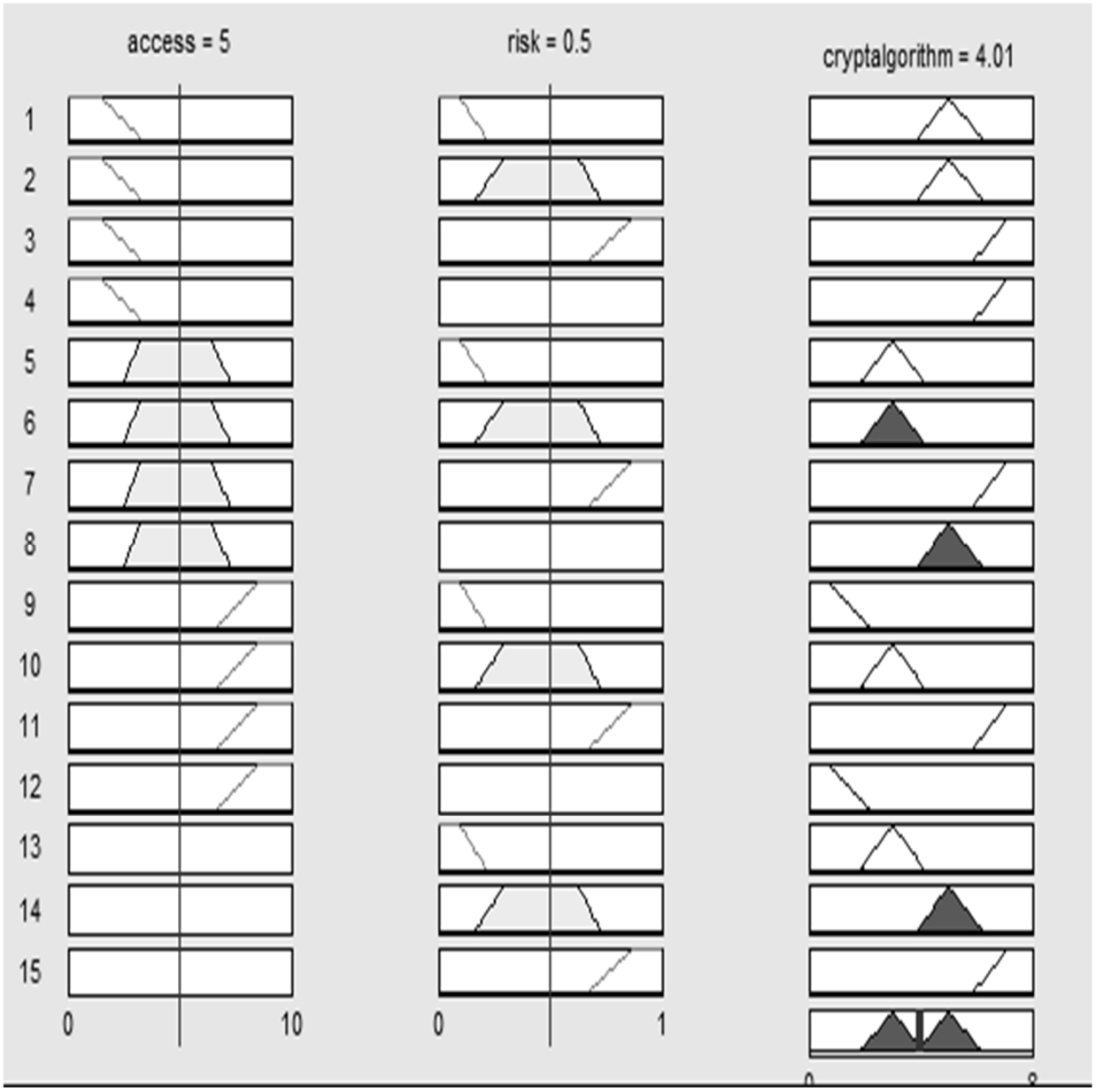


Рисунок 3.7 - База правил нечіткої системи вибору криптоалгоритму

Поверхня значень розробленої нечіткої системи вибору алгоритму захисту інформації в телемедицині зображена на рисунку 3.8.

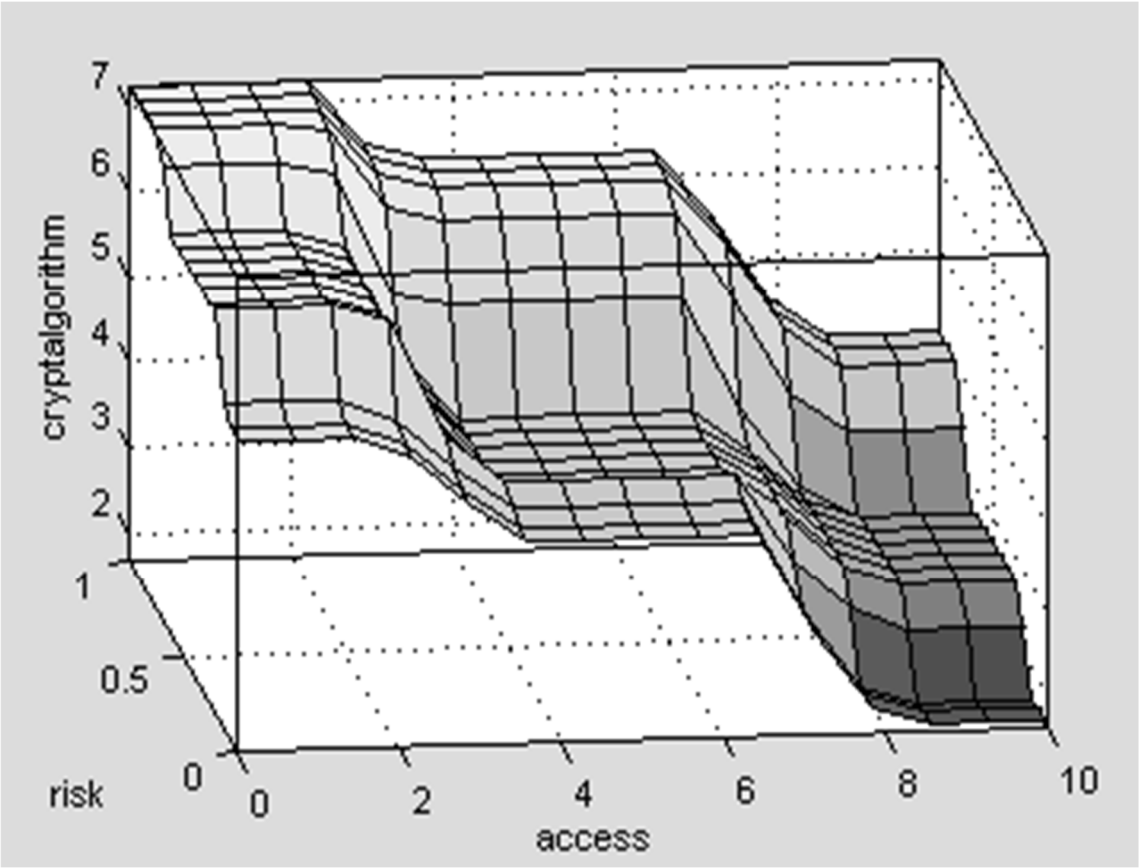


Рисунок 3.8 - Поверхня значень нечіткої системи вибору криптоалгоритму

Дослідження бази правил (див. рисунок 3.7) та поверхні значень (див. рисунок 3.8) запропонованої нечіткої системи показали правильність її роботи.

MatLab код даної нечіткої системи поданий в додатку А.

Програмна реалізація дозволяє легке та економне впровадження нечіткої системи в сервер, проте, не забезпечує захисту самої розробленої системи від несанкціонованого доступу. Тому варто реалізувати дану нечітку систему апаратно. Це можна зробити засобом Simulink середовища MatLab.

3.4 Апаратна реалізація нечіткої системи захисту інформації в телемедицині

Важливим застосуванням теорії нечітких множин є контролери нечіткої логіки, які використовуються у різноманітних системах керування, зокрема у побутових приладах. Замість математичної моделі для опису системи такі контролери використовують інтегровані знання експертів, які за структурою подання наближаються до розмовної мови і описуються за допомогою лінгвістичних змінних та нечітких множин [9 – 12]. Загальна структура fuzzi-контролера містить у своєму складі такі складові: блок фазифікації; база знань; блок рішень; блок дефазифікації. Блок фазифікації перетворює чіткі величини, виміряні на виході об'єкта керування, на нечіткі величини, описані лінгвістичними змінними у базі знань. Блок рішень використовує нечіткі умовні (if – then) правила, закладені у базі знань, для перетворення нечітких вхідних даних на необхідні керуючі впливи, що мають також нечіткий характер. Блок дефазифікації перетворює нечіткі дані з виходу блоку рішень на чітку величину, яка подається на виконавчий пристрій для керування об'єктом. Модель нечіткої системи розподілу доступу в телемадицині, що працює за класичним механізмом Мамдані, подана на рисунку 7.

Входами нечіткого контролера (Fuzzy Logic Controller), який працює за механізмом Мамдані є значення рівня доступу клієнта до інформації (access) та ризик виникнення атаки при передачі інформації поточному клієнту (risk), а виходом – значення центра ваги, який інтерпретує криптоалгоритм (cryptoalgorythm). Загальна схема нечіткого контролера містить три блоки опису функцій належності вхідних змінних (блоки Input MF), блок опису функцій належності виходу (Output MF), виходи яких поступають на вхід 15 правил (блоки Rule 1 … 15).

Загальна схема нечіткого контролера має вигляд, зображений на рисунку 3.9.

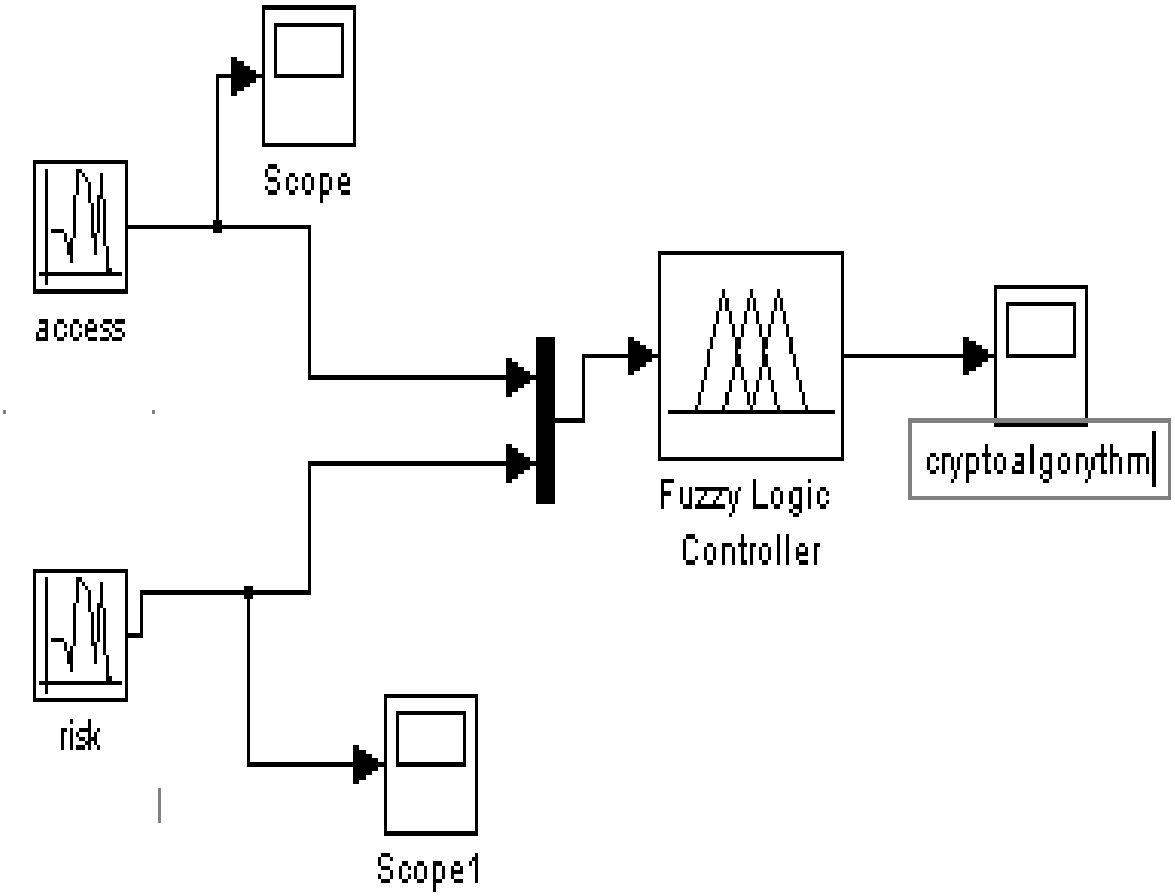


Рисунок 3.9 – Загальна схема розробленого нечіткого контролера

Основними складовими такої схеми є вхідні блоки рівня доступу та рівня ризику, які задані випадковим чином. Сам нечіткий контролер працює на основі нечткої системи. Описаної вище.

Схема роботи нечіткого контролера подана на рисунку 3.10.

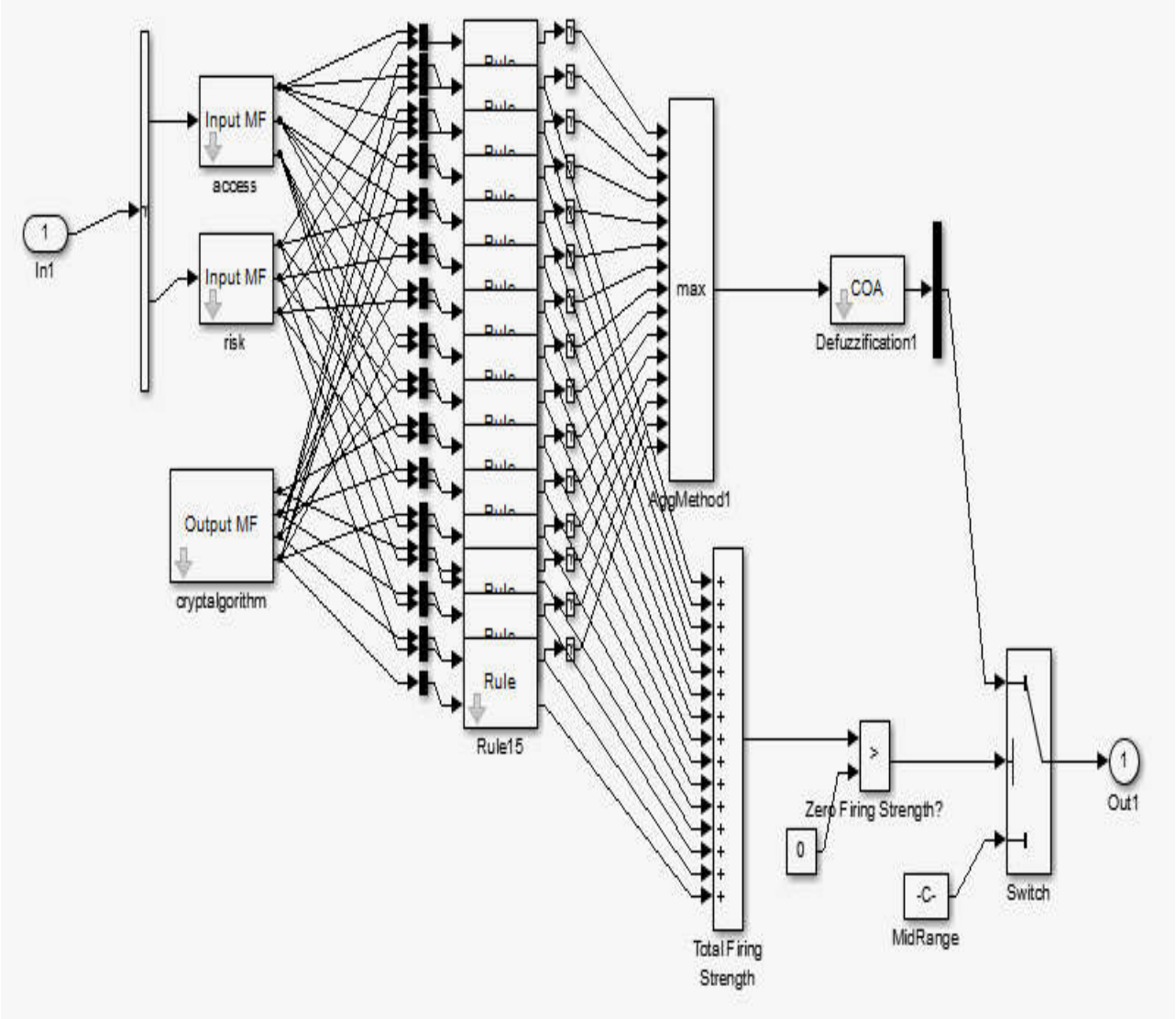
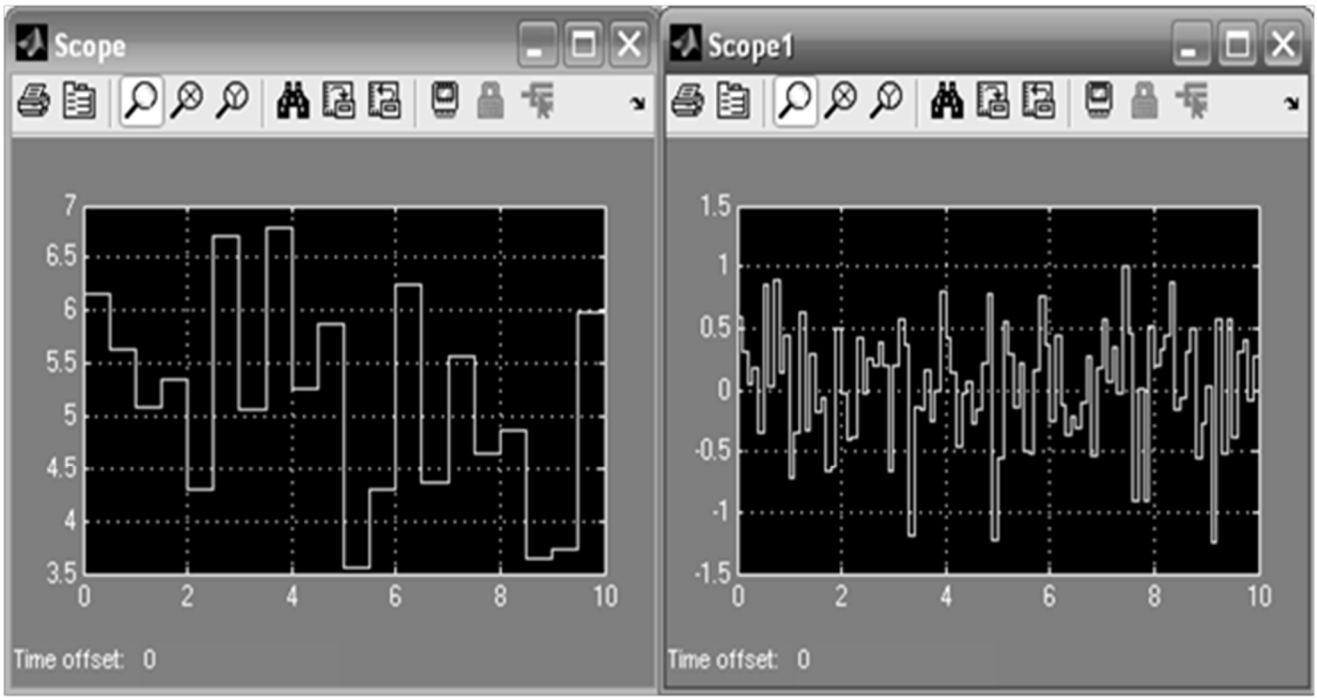


Рисунок 3.10 – Схема розробленого нечіткого контролера

Для перевірки правильності роботи розробленого нечіткого контролера необхідно проаналізувати значення вихідної змінної залежно від значень вхідних змінних. Для цього використовуються блоки Scope бібліотеки Simulink.

В даній схемі чітко відображаються 15 правил типу «якзо-то» з нечіткої бази знань розробленої системи.

Вхідні змінні задаються випадковим чином з рівномірним розподілом, що зображено на рисунку 3.11.



а) б)

Рисунок 3.11 - Рівномірно розподілене задання випадкових значень вхідних змінних: а) рівня доступу; б) ризику атаки

Схема однієї з вхідних змінних, зокрема змінної *access*, зображена на рисунку 3.12.

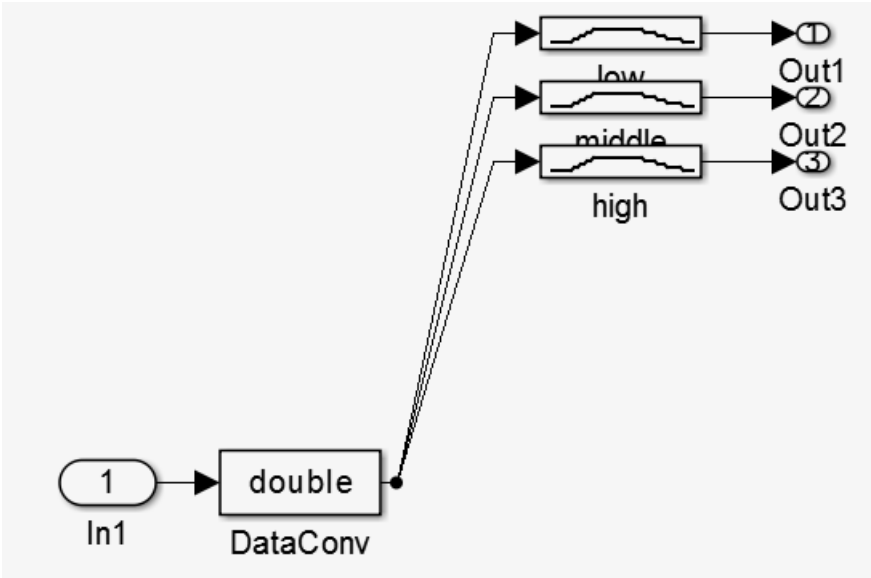


Рисунок 3.12 – Схема опрацювання вхідної змінної

Середовище Simulink зображує вихідну змінну у дещо спрощеному вигляді (рисунок 3.13).

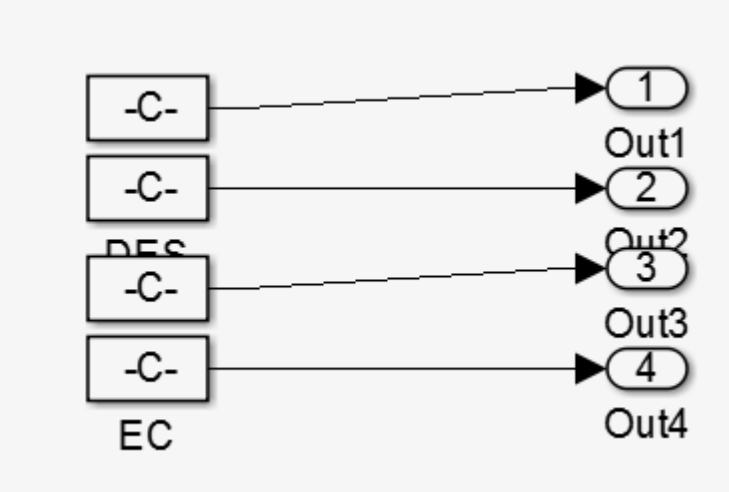


Рисунок 3.13 – Схема вихідної змінної

Значення вихідної змінної, які відповідають зазначеним на рисунку 3.5 значенням вхідних змінних, подано на рисунку 3.14.

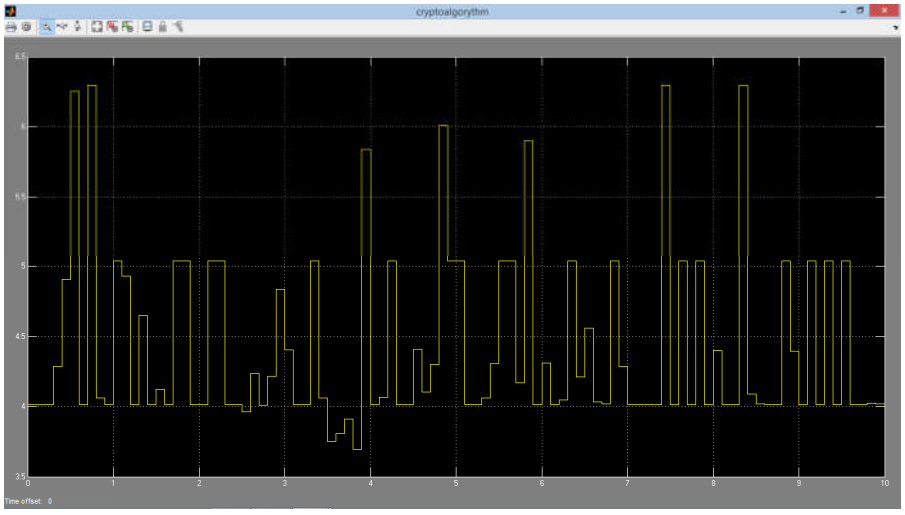


Рисунок 3.14 - Значення вихідної змінної розробленої нечіткої системи

Схема обчислення функцій належності вхідних та вихідної змінних, побудована системою Simulink, подано на рисунку 3.15.

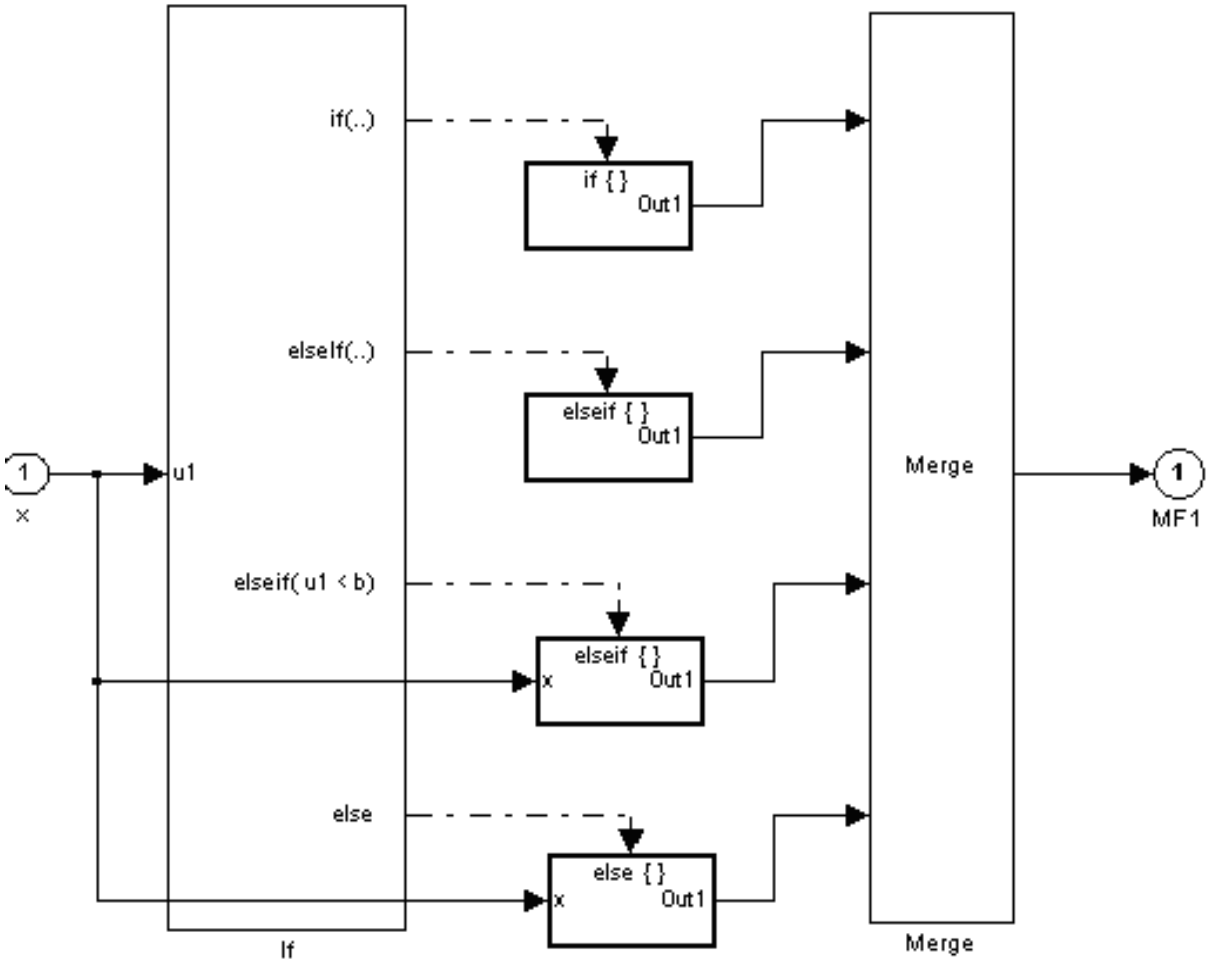


Рисунок 3.15 - Схема визначення функцій належності вхідних і вихідної змінних нечіткого контролера

Simulink опрацьовує правила з бази знань, враховуючи рейтинг, що відображається константою Weight на рисунку 3.16. Входами правила є значення вхідних змінних доступу та ризику атаки (вхід 1) та відповідне їм значення криптоалгоритму (вхід 2). Опрацювання цих даних відбувається за мінімальним законом (блок min). Виходами даної схеми є значення функції належності виходу *cryptoalgorythm* (вихід 1) та послідовність, що відображає інтервал задання цього виходу (вихід 2).

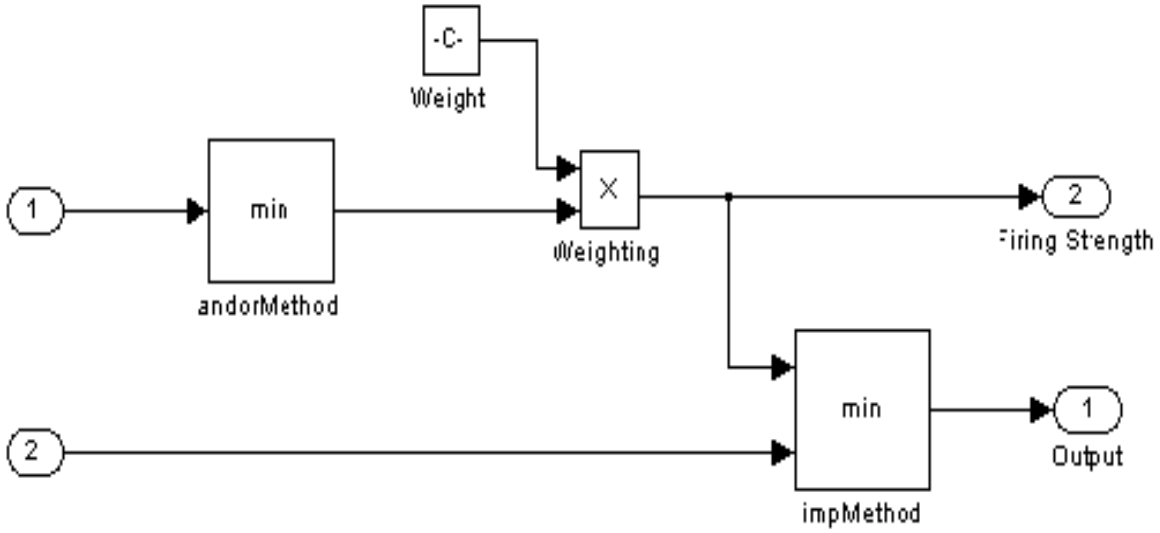


Рисунок 3.16 - Схема опрацювання вхідних нечітких значень за правилом типу «якщо - то»

Для здійснення висновку за механізмом Мамдані нечіткий контролер здійснює дефазифікацію, тобто знаходження центру ваги кінцевої фігури, що утворюється в результаті сумування виходів 15 правил. Схема дефазифікації, подана на рисунку 3.17, реалізує формулу [7]:

$$r_{öâ} = \frac{\sum_{j=1}^{m} r_j \mu(r_j)}{\sum_{j=1}^{m} \mu(r_j)},$$

де m - кількість прямокутників, на які поділено кінцеву фігуру, r_j - значення абсциси, $\mu(r_j)$ - значення ординати j -ї фігури.

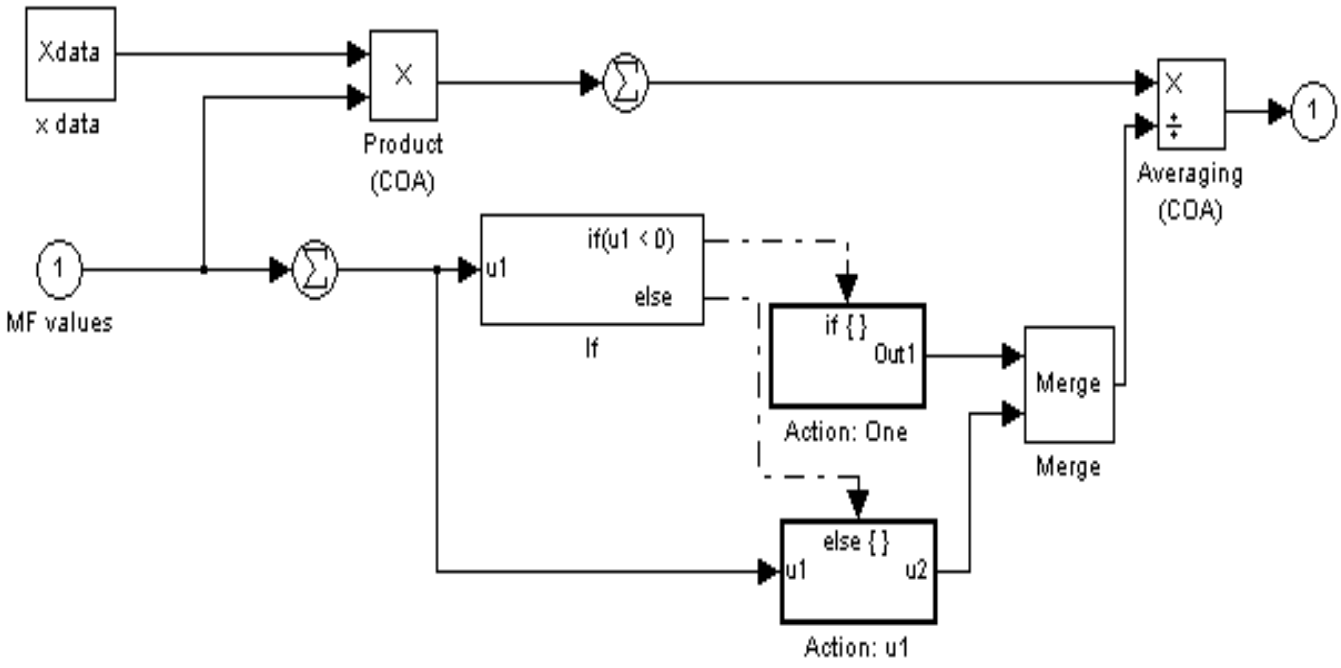


Рисунок 3.17 - Схема дефазифікації нечіткого висновку

У таблиці 3.1 подано тестові значення вхідних та вихідних значень нечіткої системи вибору оптимального криптоалгоритму за механізмом Мамдані.

Таблиця 3.1 - Тестові значення змінних побудованої нечіткої системи

№п\п	Access	Risk	Cryptoalgorythm
1	5	0.5	4.01
2	6.93	0.768	5.36
3	0.6	0.5	6.29
4	8.67	0.08	1.74
5	3.81	0.941	6.31

Аналіз результатів, поданих в таблиці 3.1 підтверджують правильність роботи розробленого засобу.

В результаті проведених досліджень розроблено нечітку систему вибору крипто алгоритму для кожного поточного клієнта телемедицини, а також реалізовано її апаратно за допомогою середовища проектування Matlab, а також доведено її працездатність, що дає змогу успішно її застосовувати на практиці.

ВИСНОВКИ

Під час дипломного проектування:

1) здійснено аналіз сучасного стану телемедицини в Україні, що дало можливість визначити основні її переваги та недоліки;

2) на основі аналізу політики захисту в сучасних телемедичних системах визначено основнметоди та засоби забезпечення стійкості медичної інформації;

3) здійснено аналіз аналіз даних в телемедичній системі, що дозволило розробити основні підходи до їх захисту;

4) розроблено основні підходи до управління доступом до конфіденційної інформації телемедицини, що дась можливість розробки адекватної політики захисту;

5) здійснено розробку та верифікацію нечіткої системи вибору алгоритму захисту інформації в телемедичній системі, що дозволить реалізувати політику захисту залежно від поточного стану системи, даних, що захищаються, та відповідно до поточного користувача телемедицини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Комп’ютерна схемотехніка: навч. посіб. / Бабич М.П., Жуков І.А., Колонтаєвський Ю.П. та ін. К.: МК-Прес, 2004. 412 с.
2. Баранов С.И. Синтез микропрограммных автоматов. Л.: Энергия, 1979. 232 с.
3. Методичні рекомендації до виконання магістерської роботи з освітнього ступеня “Магістр”. Спеціальність: 123 - Комп’ютерна інженерія. Магістерська програма - Комп’ютерна інженерія" / О.М. Березький, Л.О. Дубчак, Г.М. Мельник, Ю.М.Батько /Під ред. О.М. Березького – Тернопіль: ТНЕУ, 2019.– 43 с.
4. Методичні вказівки до оформлення курсових проектів, звітів про проходження практики, випускних кваліфікаційних робіт для студентів спеціальності «Комп’ютерна інженерія» / І.В.Гураль, Л.О.Дубчак / Пір ред. О.М.Березького. Тернопіль: ТНЕУ, 2019. 33 с.
5. Аналіз та розробка алгоритмів, методичні рекомендації./ А.В. Налімов. Барнаул, 2001. 235 с.
6. Панасенко С.П. Алгоритми шифрування. Спеціальний довідник. СПб.: БХВ-Петербург, 2009. 576 с.
7. ГОСТ 7.1-84. Библиографическое описание документа. Общие требования и правила составления. [Взамен ГОСТ 7.1-76; Введ.01.01.86]. М.: Изд-востандартов, 1984. 78с.
8. ДСТУ 3008-95. Державний стандарт України. Документація. Звіти у сфері науки і техніки. Структура і правила оформлення. [Введ. 23.02.95] К.: Держстандарт України, 1995. 37 с.
9. Шнайер Б. Генератори псевдовипадкових послідовностей і потокові шифри // Прикладна криптографія. 2002. 816 с
10. VHDL Tutorial: Learn by Example: веб-сайт. URL:http://esd.cs.ucr.edu/labs/tutorial/ (дата звернення: 12.10.2018).

11. SerialandUARTTutorial: веб-сайт. URL: https://freebsd.org/doc/en/articles/ (дата звернення: 10.04.2019)

12. AVRandUART – Tutorial: веб-сайт. URL: http://electroschematics.com/ (дата звернення: 07.06.2019)

13. Вербіцький О.В. Вступ до криптографії. Львів: Видавництво науково-технічної літератури, 1998. 247 с.

14. Сучасна криптографія. Основні поняття. / В. Ємець, А. Мельник, Р. Попович. Львів: БаК, 2003. 144 с.

15. Криптография / А.А. Молдовян, В.А.Молдовян и др. Серия “Учебники для вузов. Специальная литература”. Спб.: Издательство “Лань”, 2000. 224 с.

16. Столлингс В. Криптография и защита сетей: принципы и практика. М.: Изд. Дом «Вильямс», 2001. 672 с.

17. Чмора А.Л. Современная прикладная криптографія. М.: Гелиос АРВ, 2002. 256 с.

18. А.Я.Горпенюк, В.Б.Дудикевич, І.Б.Ломницький. Підвищення швидкодії при обчисленні важкооборотних функцій в асиметричних алгоритмах шифрування. Захист інформації. 2003. №1(18). С.36-43.

19. Построение и анализ вычислительных алгоритмов / А.Ахо, Дж.Хопкрофт, Дж.Ульман. М.: Мир, 1979. 325 с.

20. Варновский Н.П. Криптография и теория сложности. Математическое просвещение. Сер. 3, №2, 1998. С. 71-86.

21. Брассар Дж. Современная криптология. М.: Мир ПК, 1997. 132 с.

22. Ивченко В.Г. Применение VHDL при проектировании СБИС. Спб.: Техпринт, 2003. 342 с.

23. Инструментальные средства обеспечения безопасности. / Джонс К.Д., Шема М., Джонсон Б.С. М.: ИНТУИТ, 2007. 128 с.

24. Ивченко В.Г. Применение VHDL при проектировании СБИС. К.: МК-Прес, 2007. 256с.

25. Бабило П.Н. Системы проектирования интегральных схем на основе языка VHDL. StateCAD, ModelSim, LeonardoSpectrum. М.: ИНТУИТ, 2005. 384 с.

26. Бабило П.Н. Основы языка VHDL: Учебное пособие. Издание 5-е. М.: ИНТУИТ, 2012. 328 с.

27. Кунву Лі. Основи САПР (CAD/CAM/CAE). М.: ИНТУИТ, 2004. 560 с.

28. Berezsky O. Fuzzy system diagnosing of precancerous and cancerous conditions of the breast / O. Berezsky, S. Verbovyy, L. Dubchak, T. Datsko - XIth International Scientific and Technical Conference "Computer Sciences and Information Technologies (CSIT), 2016. Pp.200-203.

29. Berezsky O. Fuzzy System of Diagnosing in Oncology Telemedicine / Berezsky O., Verbovyy S., Dubchak L., Datsko T. Sensors & Transducers. Jan 2017. Pp. 32-38.

30. Штовба С.Д. Обеспечение точности и прозрачности нечеткой модели Мамдани при обучении по экспериментальным данням. Проблемы управления. 2007. №4. С. 102-104.

31. Дубчак Л.О. Метод обробки нечітких даних на основі механізму Мамдані. Системи обробки інформації. 2012. №7(105). 131с.

32. Дубчак Л.О. Спосіб обробки нечіткої інформації. Вісник Східноукраїнського національного університету ім. В.Даля. 2012. №8(179)Ч.1. С.306-309.

33. M.S.Abadeh, J.Habibi, C.Lucas. Intrusion Detection Using a Fuzzy Genetics-Based Learning Algorithm. Journal of Network and Computer Applications. 2007. №30. P.414-428.

34. Ross T.J. Fuzzy Logic with Engineering Applications. McGraw-Hill Inc.(USA), 1995. 600 p.

35.Васильцов І.В.Атаки спеціального виду на криптопристрої та методи боротьби з ними / За ред. В.П.Широчина. Кременець: Видавничий центр КОГПІ, 2009. 264 с.

36.Комп'ютерні мережі: Підручник. / Ю.О.Кулаков, Г.М.Луцький / За ред. Ю.С.Ковтанюка. К.: Видавництво «Юніор», 2005. 400 с.

37.Защита информации в компьютерных системах и сетях / Под ред. В.Ф.Шаньгина / Ю.В.Романец, П.А.Тимофеев, В.Ф.Шаньгин. М.: Радио и связь, 1999. 328 с.

38.Вопросы проектирования механизмов защиты информации в компьютерных системах и сетях / В.П.Широчин, В.Е.Мухин, А.В.Кулик. К.: “ВЕК+”, 2000. 112 с.

39.Розробка клієнт-орієнтованих засобів шифрування абонентських даних в мобільному зв’язку / В.Б.Дудикевич, Ю.Л.Пархуць // Інформаційна безпека. – 2011. №1(5). С.83-87.

40.Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. М.: Изд. Дом «Вильямс», 2001. 672 с.

41.Безмалый Н.В. Как ломаются пароли. Журнал информационных технологий CHIP. 2008. №7. С.124-126.

42.Україна значно піднялася в рейтингу країн з найбільшою кількістю кібер-загроз: веб-сайт. URL: http://www.rbc.ua/ukr/top/show/ (дата звернення 25.12.2018).

43.Штовба С.Д. Введение в теорию нечетких множеств и нечеткую логику: веб-сайт. URL: http://matlab.exponenta.ru/fuzzylogic/book1/ (дата звернення 25.12.2018)

44.Штовба С.Д. Обеспечение точности и прозрачности нечеткой модели Мамдани при обучении по экспериментальным данным. Проблемы управления и информатики. 2007. №4. С. 102–114.

45.Бережная М.А. Методы проектирования нечетких устройств принятия решений на основе программируемых логических интегральных микросхемах. Технология приборостроения. 2009. №2. С. 16–23.

46.Использование нечеткой адаптивной системы управления для компьютерного мониторинга сетью котельных установок / В.С.Михайленко, В.В.Никольский: веб-сайт. URL: http://aaecs.org/mihailenko-vs-nikolskii-vv-

ispolzovanie-nechetkoi-adaptivnoi-sistemi-upravleniya-dlya-kompyuternogo-monitoringa-setyu-kotelnih-ustanovok.html (дата звернення 25.12.2018)

47.Intrusion detection by integrating boosting genetic fuzzy classifier and data mining criteria for rule pre-screening. T.Ozyer, R.Alhajj, K.Barker. Journal of Network and Computer Applications. 2007. №30. P.99-113.

48.Корченко А.Г. Построение систем защиты информации на нечетких множествах : Теория и практические решения. К.: МК-Пресс, 2006. 320 с.

49.Гнатчук Є.Г. Інформаційна технологія подання та опрацювання знань на основі нечіткої логіки в експертних системах діагностування комп'ютерних засобів: автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.13.06 «Інформаційні технології». Львів, 2008. 20 с.

50. Computer diagnostic tools based on biomedical image analysis / O. Berezsky, O. Pitsun, S. Verbovyy, T. Datsko, A. Bodnar - XIV-th of the International Conference on The Experience of Designing and Application of CAD Systems in Microelectronics, CADSM'2017. Pp. 388-391.

Додаток А

MATLAB код нечіткої системи вибору криптоалгоритму

```
[System]
Name='telemedycyna'
Type='mamdani'
Version=2.0
NumInputs=2
NumOutputs=1
NumRules=15
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'
 [Input1]
Name='access'
Range=[0 10]
NumMFs=3
MF1='low':'trapmf',[-3.6 -0.4 1.49 3.32010582010582]
MF2='middle':'trapmf',[2.53 3.24 6.38888888888889 7.29]
MF3='high':'trapmf',[6.65 8.505291005291 10.4 13.6]
 [Input2]
Name='risk'
Range=[0 1]
NumMFs=3
MF1='low':'trapmf',[-0.36 -0.04 0.0939153439153439 0.22]
MF2='middle':'trapmf',[0.163 0.295 0.628306878306878 0.726]
MF3='high':'trapmf',[0.672 0.863756613756614 1.07 1.33]
```

[Output1]

Name='cryptalgorithm'

Range=[0 8]

NumMFs=4

MF1='none':'trapmf',[-2.88 -0.32 0.709 2.19047619047619]

MF2='DES':'trimf',[1.83 3 4.15873015873016]

MF3='RSA':'trimf',[3.9 5 6.21]

MF4='EC':'trapmf',[5.89417989417989 7.08 8.01 8.62]

[Rules]

1 1, 3 (1) : 1

1 2, 3 (1) : 1

1 3, 4 (1) : 1

1 0, 4 (1) : 1

2 1, 2 (1) : 1

2 2, 2 (1) : 1

2 3, 4 (1) : 1

2 0, 3 (1) : 1

3 1, 1 (1) : 1

3 2, 2 (1) : 1

3 3, 4 (1) : 1

3 0, 1 (1) : 1

0 1, 2 (1) : 1

0 2, 3 (1) : 1

0 3, 4 (1) : 1