Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

ОЛЕШКО ІННА ВІКТОРІВНА

УДК 004.056.53

МОДЕЛІ ТА МЕТОДИ ОЦІНКИ ЗАХИЩЕНОСТІ МЕХАНІЗМІВ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

05.13.21 – системи захисту

Автореферат дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2014

Дисертацією є рукопис.

Робота виконана у Харківському національному університеті радіоелектроніки Міністерства освіти і науки України.

Науковий керівник доктор технічних наук, професор
Горбенко Іван Дмитрович,
Харківський національний університет ім. В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій.

Офіційні опоненти: доктор технічних наук, професор
Харченко Вячеслав Сергійович,
Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», завідувач кафедри комп'ютерних систем та мереж;

кандидат технічних наук, доцент
Проскуровський Роман Васильович,
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут", заступник завідувача кафедри застосування засобів криптографічного та технічного захисту інформації.

Захист відбудеться « 8 » квітня 2014 р. о 13.00 годині на засіданні спеціалізованої вченої ради К 64.052.05 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

З дисертацією можна ознайомитися в бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

Автореферат розісланий « » 2014 р.

Вчений секретар
спеціалізованої вченої ради І. В. Лисицька

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Забезпечення безпеки інформаційної системи є одним з найважливіших завдань в ході її експлуатації, оскільки від конфіденційності, цілісності та доступності інформаційних ресурсів багато в чому залежить швидкість прийняття рішень, ефективність і надійність роботи. Зараз для будь-якої компанії або приватної особи, яким потрібно захищати дані, як ніколи важливі безпека і перевірка автентичності. Використання механізмів простої автентифікації підприємствами та організаціями певною мірою вичерпує себе. Продовжуючи використовувати цей традиційний механізм доступу щодо власних інформаційних ресурсів, компанії фактично ставлять під загрозу рентабельність та існування підприємства. Незважаючи на безліч засобів обчислювальної техніки і широкий спектр технологічних рішень, вибір методів автентифікації для компаній, що планують своє майбутнє, не великий – швидше за все, необхідно використовувати механізми багатофакторної автентифікації. Багатофакторною автентифікацією називають автентифікацію з хоча б двома незалежними факторами автентифікації. При цьому можуть використовуватися фактори різної природи:

• Властивість, яку має суб'єкт. Наприклад, біометрія, тобто природні унікальні відмінності особи: обличчя, відбитки пальців, райдужна оболонка ока, капілярні візерунки, послідовність ДНК тощо.

• Знання – інформація, яку знає суб'єкт. Наприклад, пароль чи пін - код.

• Володіння – річ, яку має суб'єкт. Наприклад, електронна або магнітна картка, флеш - пам'ять, електронний ключ.

Сильні і слабкі сторони багатофакторної автентифікації, загалом, відомі. До її переваг можна віднести здатність захистити інформацію, як від внутрішніх загроз, так і від зовнішніх вторгнень. Певною слабкістю можна вважати необхідність використання додаткових програмно - апаратних комплексів, засобів зберігання і зчитування даних. Методам захисту, заснованих на механізмах багатофакторної автентифікації, сьогодні довіряє багато зарубіжних компаній, серед яких високотехнологічні компанії фінансового та страхового секторів ринку, великі банківські установи та підприємства держсектора, незалежні експертні організації, дослідницькі фірми тощо. Водночас, зараз статистика зломів систем, які застосовують багатофакторну автентифікацію, відсутня або незначна. Тому, на наш погляд, важливим питанням є оцінка безпеки схем багатофакторної автентифікації. В процесі побудови системи захисту від НСД (несанкціонованого доступу) спочатку необхідно визначити перелік факторів, які можна застосувати для здійснення багатофакторної автентифікації. Для захисту від НСД інформації та ресурсів з використанням певних факторів автентифікації необхідно визначити повний перелік атак зі сторони існуючих чи потенційних криптоаналітиків (порушників), зробити їх класифікацію, вибрати критерії та показники, які дозволили б їх порівняти та вибрати такі атаки, які можуть бути реалізовані та забезпечували б досягнення максимальних значень ймовірностей НСД.

Зв’язок роботи з науковими програмами, темами. Дисертаційна робота виконана в рамках: держбюджетної НДР № 262-1 від 01.01.2011 р. «Розвиток, стандартизація, уніфікація, удосконалення та впровадження інфраструктури

відкритих ключів (включаючи національну систему електронного цифрового підпису) на внутрішньодержавному та міжнародному рівнях» за наказом МОНУ № 1177 від 30.11.2010 р. (ДР № 0111U002628); госпдоговірної НДР № 11-06 від 01.03.2011 р. «Розробка методів, комплексів та засобів ІВК для національних та міжнародних інформаційно-телекомунікаційних систем та інформаційних технологій» (ДР № 0111U002634), держбюджетної НДР № 275-1 «Аналіз стану, визначення напрямів розвитку, стандартизація, удосконалення, розробка та впровадження криптографічних систем, включаючи систему ЕЦП» (ДР № 0113U000363).

Мета та задачі дослідження. Метою досліджень є розробка математичних моделей і методів оцінки захищеності від НСД інформації та ресурсів з використанням механізмів багатофакторної автентифікації й порівняльний аналіз механізмів багатофакторної автентифікації, що дозволяє мінімізувати ймовірності НСД щодо інформації та ресурсів.

Для досягнення поставленої мети в роботі вирішено такі основні задачі:

1. Розробка ентропійної моделі райдужної оболонки ока, обчислення на її основі кількості інформації, яка міститься в райдужці, порівняльний аналіз кількості інформації, яка міститься в райдужці із кількістю біометричної інформації, що міститься в обличчі.

2. Розробка моделі загроз та обґрунтування критеріїв та показників оцінки захищеності ІТС (інформаційно - телекомунікаційна система) від НСД.

3. Теоретичне обґрунтування та розробка математичних моделей оцінки захищеності від НСД інформації та ресурсів з використанням механізмів багатофакторної автентифікації, включаючи комбіновані трифакторні та двофакторні схеми, а також послідовні двофакторні та трифакторні структури.

4. Обґрунтування та удосконалення криптографічного протоколу нульових знань, що базується на перетвореннях у скінченому полі шляхом переведення його в групу точок еліптичної кривої.

5. Аналіз апаратно-програмних засобів автентифікації за критерієм захищеності від НСД.

6. Розробка методів оцінки захищеності від НСД з використанням механізмів багатофакторної автентифікації. Для кожного із факторів визначити повний перелік атак зі сторони існуючих чи потенційних криптоаналітиків (порушників), зробити їх класифікацію, вибрати критерії та показники, які дозволяють їх порівняти та вибрати такі атаки, які можуть бути реалізовані та забезпечували б максимальні значення ймовірностей НСД. Основною оцінкою степені захищеності є ймовірність НСД та безпечної автентифікації.

7. Розробка програмних моделей, що реалізують обчислення кількості біометричної інформації райдужної оболонки ока для різних алгоритмів, а також програмне моделювання удосконаленого протоколу нульових знань.

Об'єктом дослідження є процеси оцінки захищеності від НСД інформації та ресурсів з використанням механізмів багатофакторної автентифікації.

Предметом досліджень є математичні моделі та методи оцінки захищеності від НСД інформації й ресурсів з використанням механізмів багатофакторної автентифікації.

Методи досліджень: теорія автентифікації – для розробки ентропійної моделі біометричної автентифікації; теорія надійності – для оцінки ймовірності НСД та безпечної автентифікації; теорія асиметричних криптоперетворень – для оцінки захищеності від НСД, коли як фактор автентифікації використовуються асиметричні пари ключів; програмного моделювання – для реалізації удосконаленого протоколу нульових знань та для обчислення біометричної інформації обличчя та райдужної оболонки ока.

Наукова новизна одержаних результатів полягає у тому, що:

1. Вперше запропоновано математичні моделі оцінки захищеності від НСД інформації та ресурсів з використанням механізмів багатофакторної автентифікації, які базуються на обчисленні ймовірностей НСД та безвідмовної роботи механізмів, що дозволяє оцінити ймовірності НСД у схемах багатофакторної автентифікації.

2. Удосконалено метод автентифікації, який описано в стандарті ДСТУ ISO/IEC 9798-5, що відрізняється від існуючого тим, що замість перетворень в мультиплікативній групі поля використовуються перетворення у групі точок еліптичної кривої, що дозволяє досягти експоненційного рівня складності здійснення атаки «повне розкриття», а також зменшити довжини ключа при збереженні показника безпечного часу.

3. Вперше запропоновано методи оцінки захищеності від НСД з використанням механізмів багатофакторної автентифікації, які базуються на визначенні повного переліку атак відносно аналізованого фактора, їх класифікації, аналізу критеріїв та показників, які дозволяють їх порівняти та вибору таких атак, які можуть бути реалізовані та забезпечували б досягнення максимальних значень складностей криптоаналізу, що дозволяє оцінити ймовірності НСД як при використанні кожного фактора окремо, так і в схемах багатофакторної автентифікації взагалі.

4. Вперше запропоновано ентропійну модель райдужної оболонки ока, яка базується на визначенні кількості інформації, яка міститься в райдужній оболонці, що дозволяє обчислити кількість біометричної інформації райдужки та порівнювати не тільки біометричні ознаки між собою, але і з персональним ідентифікаційним номером (ПІН), паролем та іншими методами автентифікації в ході використання їх ентропійних оцінок.

Практичне значення отриманих результатів.

1. На основі розробленої ентропійної моделі райдужної оболонки ока розраховано кількість біометричної інформації, яка міститься в райдужній оболонці ока і зроблено порівняльний аналіз із біометричною інформацією, яка міститься в обличчі. Кількість біометричної інформації для обличчя складає 45 біт, а для райдужки – 288 біт. Таким чином, метод розпізнавання на основі райдужної оболонки ока дозволяє більш надійно виконувати автентифікацію особи.

2. Зроблено порівняльний аналіз методів біометричної автентифікації на основі помилок першого і другого роду. На основі проведеного аналізу, можна зробити висновок про те, що найбільш точним і найкращим методом біометричної автентифікації є автентифікація за райдужною оболонкою ока (помилка першого роду для нього складає $1*10^{-6}$). Як додатковий параметр, можна використовувати відбиток пальця або геометричну форму кисті руки.

3. Розроблено програмні моделі, які реалізують запропонований метод за обчисленням кількості біометричної інформації, що міститься в райдужній оболонці ока для різних алгоритмів, а також виконано програмне моделювання удосконаленого протоколу нульових знань.

4. Зроблено порівняльний аналіз існуючого протоколу нульових знань, описаного в стандарті ДСТУ ISO/IEC 9798-5 та удосконаленої його версії на основі методу аналізу ієрархій. Результуючий вектор значущості має такі значення: для удосконаленої версії $\approx 0{,}7$, а для існуючого протоколу $\approx 0{,}3$. Таким чином, кращим протоколом автентифікації визнано удосконалений протокол, заснований на перетвореннях у групі точок еліптичної кривої.

5. На основі запропонованого методу оцінки захищеності від НСД з використанням механізмів багатофакторної автентифікації отримано значення ймовірностей НСД, коли як фактор автентифікації використовуються асиметричні пари ключів, паролі або біометричні ознаки, а також значення ймовірностей НСД для двофакторних та трифакторних систем автентифікації. Найбільш захищеним механізмом багатофакторної автентифікації є механізм, у якому використовуються три фактори автентифікації, наприклад: біометрія, ключ та пароль.

Особистий внесок здобувача. Всі основні результати отримано автором особисто. В роботах, що написані у співавторстві, автору належить: [1] – оцінки захищеності від НСД для двофакторної та трифакторної схем автентифікації, модель послідовно-паралельного механізму «пароль-ключ-біометрія»; [2] – обчислення біометричної інформації райдужної оболонки ока та порівняльний аналіз із біометричною інформацією обличчя; [4] – аналіз методів біометричної автентифікації та їх класифікація, порівняльний аналіз систем біометричної автентифікації на основі помилок першого та другого роду; [5] – аналіз основних протоколів суворої автентифікації, порівняльний аналіз протоколів суворої автентифікації на основі умовних та безумовних критеріїв.

Апробація результатів дисертації Основні результати дисертаційної роботи були представлені, доповідалися й обговорювалися на міжнародних і всеукраїнських науково-технічних конференціях, зокрема на: 1) XI-й Міжнародній науково-технічній конференції «АВІА-2013», м. Київ, 2013; 2) Науково-технічній конференції із міжнародною участю «Компьютерное моделирование в наукоемких технологиях» (КМНТ-2012), м. Харків, 2013; 3) VI-й Міжнародній науково-практичній конференції «Наука и социальные проблемы общества: информатизация и информационные технологи», м. Харків, 2011; 4) I-й Міжнародній науково-технічній конференції «Захист інформації і безпека інформаційних систем», м. Львів, 2012; 5) XV-й Ювілейній міжнародній науково-практичній конференції «Безопасность информации в информационно-телекоммуникационных системах», Київ, 2012; 6) 15-му Ювілейному міжнародному молодіжному форумі «Радиоэлектроника и молодежь в XXI веке», м Харків, 2011; 7) XVI-й Міжнародній науково-практичній конференції «Безопасность информации в информационно-телекоммуникационных системах», Київ, 2013; 8) IV-му Міжнародному радіоелектронному форумі «Прикладная радиоэлектроника. Состояние и перспективы развития» МРФ–2011, Харків, 2011.

Публікація результатів роботи. Основні положення та результати

дисертаційної роботи опубліковано у 14 наукових працях: 5 статей, опублікованих у наукових фахових виданнях України, 1 стаття у виданні, яке входить до міжнародних наукометричних баз, а також 8 матеріалів і тез наукових конференцій.

Структура та обсяг дисертації. Дисертація складається із вступу, п'яти розділів і висновків, обсягом 218 сторінок, з яких 164 сторінки основного тексту, які містять 24 рисунки, 42 таблиці, список використаних джерел із 95 найменувань на 11 сторінках та 7 додатків на 41 сторінці.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність задач, які вирішуються у дисертаційній роботі, сформульовано мету дослідження, а також викладено наукову новизну та практичну значущість отриманих результатів.

У першому розділі дисертації розглядається стан застосування основних методів і засобів автентифікації в комп'ютерних системах та мережах. Розглядаються загальні проблеми щодо створення систем електронної ідентифікації. Відмічається, що національне законодавство України немає основ для безпечних, надійних і простих електронних операцій, що включають електронну ідентифікацію, автентифікацію і підписи. Існуюче законодавство потребує покращення, розширення та прийняття на рівні ЄС. У 2012 році ЄС прийняв Регламент щодо електронної ідентифікації та довірчих послуг для електронних операцій на внутрішньому ринку, який Україна має враховувати в ході удосконалення та розвитку національної системи надання довірчих послуг. Основою цього Регламенту є створення єдиної законодавчої бази для забезпечення електронної ідентифікації і автентифікації транскордонно.

Викладається сутність та обґрунтовуються вимоги щодо надання довірчих послуг. Робиться висновок про те, що суттєво проблемними в ЄС є задачі, пов'язані з транскордонним визнанням електронної ідентифікації та автентифікації. Ці ж задачі є суттєво проблемними і для України.

Аналізуються основні джерела в частині методів, механізмів і протоколів ідентифікації та автентифікації. Ґрунтуючись на ISO/IEC 19790:2012, зазначається, що існує чотири рівні безпеки криптографічного модуля. Найсильнішою схемою автентифікації є багатофакторна автентифікація, яка поєднує в собі використання криптографічних та біометричних методів. Тому актуальним є розроблення й аналіз саме цих схем.

Наводиться понятійний апарат у частині надання довірчих послуг. Визначаються такі поняття, як довірча послуга, кваліфікована довірча послуга, провайдер довірчих послуг, електронний підпис, електронна печатка, кваліфікована електронна мітка часу, електронний документ, послуга електронної доставки, кваліфікований сертифікат для перевірки справжності веб-сайту, ідентифікація, автентифікація.

Розділ завершується формулюванням висновків за проведеними дослідженнями, а також формулюванням задач досліджень роботи.

Другий розділ дисертації присвячено аналізу основних методів біометричної автентифікації, порівняльному аналізу методів біометричної автентифікації та

розробці ентропійної моделі райдужної оболонки ока. Порівняльний аналіз методів біометричної автентифікації проводився на основі помилки першого роду (FAR), помилки другого роду (FRR) та коефіцієнта рівної ймовірності помилок (EER). Також враховувались переваги і недоліки біометричних методів. Результати порівнянь наведені в таблиці 1.

Таблиця 1 – Порівняльний аналіз методів біометричної автентифікації

Біометричний параметр	**Помилка I роду (FRR)**	**Помилка II роду (FAR)**	**Значення EER у %**
Відбиток пальця	0,01 - 0,0001	0,002 - 0,0001	0,01
Геометрія кисті руки	0,001	0,000001	0,1-0,5
Райдужна оболонка ока	0,009	$1*10^{-6}$	0,0021
Тримірне зображення обличчя	0,103	0,0047	0,75

На основі проведеного аналізу, можна зробити висновок про те, що найбільш точним і найкращим методом біометричної автентифікації є автентифікація за райдужною оболонкою ока. Як додатковий параметр, можна використовувати відбиток пальця або геометричну форму кисті руки.

Для обчислення біометричної інформації райдужної оболонки ока використовувалась база даних CASIA. Зображення райдужної оболонки було попередньо оброблено за алгоритмом Libor Masek. Результати процесу передобробки зображення наведені на рис. 1.

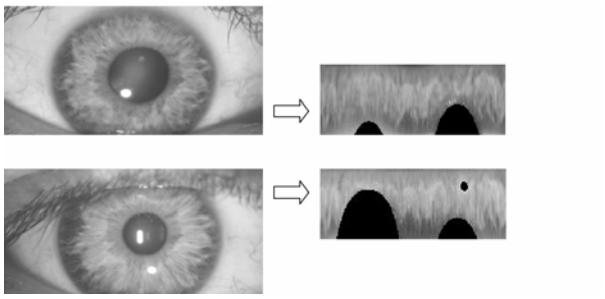

Рисунок 1 – Результати процесу передобробки зображення райдужки

Далі для кожного ока формується вектор біометричних характеристик. Так, для людини f ми маємо N_f зразків характеристик райдужної оболонки ока, в той час як для населення – N_b зразків характеристик. Визначивши x як значення випадкової величини X, обчислимо середнє зображення райдужки у населення μ_b:

$$\mu_b = \underset{b}{M}[X] = \frac{1}{N_b}\sum_{i=1}^{N_b} x_i \,. \tag{1}$$

Середнє зображення райдужки людини визначається аналогічно, замінюючи b на f. Нормалізування всіх зображень у навчальній вибірці проводиться за допомогою віднімання середнього зображення. Матриця коваріації райдужної оболонки для населення Σ_b визначається таким чином:

$$\Sigma_b = \underset{b}{M}[(X-\mu_b)^t(X-\mu_b)] = \frac{1}{N_b - 1}\sum_{i=1}^{N_b}(x_i-\mu_b)^T(x_i-\mu_b)\,, \tag{2}$$

де $x_i - \mu_b$ – нормалізоване зображення райдужної оболонки ока. Матриця коваріації для людини обчислюється аналогічно. Однією з важливих проблем під час прямих вимірювань теоретичної інформації є придатність даних. Для позбавлення від цієї проблеми перейдемо до моделі з невеликою кількістю параметрів. Використаємо для цього Гауссовий розподіл. Обчислимо розподіли біометричних характеристик людини та населення, ґрунтуючись на Гауссовій моделі і відповідних b і f:

$$f(x) = \frac{1}{\sqrt{|2\pi\Sigma_f|}} exp(-\frac{1}{2}(x-\mu_f)^t \Sigma_f^{-1}(x-\mu_f)), \tag{3}$$

$$b(x) = \frac{1}{\sqrt{|2\pi\Sigma_b|}} exp(-\frac{1}{2}(x-\mu_b)^t \Sigma_b^{-1}(x-\mu_b)). \tag{4}$$

З формул (3) та (4) обчислимо відносну ентропію $D(f||b)$:

$$D(f||b) = k(ln\frac{|2\pi\Sigma_b|}{|2\pi\Sigma_f|} + trace((\Sigma_f + T)\Sigma_b^{-1} - I)), \tag{5}$$

де $T = (\mu_f - \mu_b)^t(\mu_f - \mu_b), k = log_2\sqrt{e}$. Для позбавлення від корельованих характеристик у наших вимірах були застосовані метод головних компонент (PCA) та ICA (independent component analysis). Було обчислено 327 векторів характеристик, які використовувалися для подальшого аналізу. На рис. 2 проілюстрована біометрична інформація, обчислена для 327 PCA та ICA характеристик райдужної оболонки. Стандартне відхилення зображено внизу кожного графіка.

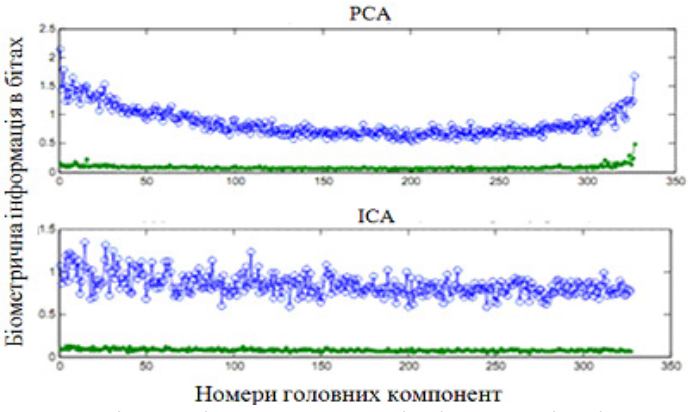

Рисунок 2 – Залежність біометричної інформації від номера вектора характеристик для PCA та ICA

Перепишемо $D(f||b)$ у PCA просторі:

$$D(f||b) = k(\beta + traceU((S_f + S_t)S_b^{-1} - I)U^T), \tag{6}$$

де $\beta = \ln\frac{|S_b|}{|S_f|}$ ma $S_t = U^T TU$, S_b – діагональна матриця власних значень, U – ортогональна матриця власних векторів, S_f – необов'язкова діагональна матриця.

Розрахуємо нижню границю для оцінки відносної ентропії. Для цього необхідно зробити такі припущення:

1. Оцінки дисперсії характеристик матриці $[S_f]_{i,i}$ дійсні для всіх i;

2. Оцінки коваріації характеристик матриці $[S_f]_{i,j}$ для i≠j дійсні тільки для найбільш важливих L характеристик, де $L< N_f$.

Характеристики, які не вважаються правильними, ґрунтуючись на цих припущеннях, встановлюються в 0 множенням S_b на маску M:

$$M = \begin{cases} 1, \textit{якщо } i = j \textit{ чи } (i < L \textit{ та } j < L) \\ 0, \textit{в інших випадках} \end{cases}. \quad (7)$$

Використовуючи алгоритм для обчислення біометричної інформації, описаний вище, і базу даних CASIA, отримуємо, що середня біометрична інформація райдужної оболонки ока для PCA головних компонент складає 278 біт, а для ICA – 288 біт. Як бачимо, кількість біометричної інформації для ICA і PCA компонент дуже близька. ICA компоненти містять більше інформації імовірно тому, що вони відповідають моделі характеристичних даних райдужки краще. Такі результати сумісні з попередніми дослідженнями райдужної оболонки ока. Так, Daugman заявляв, що комбінаторна складність фазової інформації райдужної оболонки ока різних людей становить близько 249 ступенів свободи. Cover і Thomas, використовуючи райдужку діаметром в 11мм, прорахували, що її біометрична інформація становить 241 біт. Різниця наших даних зі значеннями Daugman і Thomas можна пояснити тим, що діаметр райдужної оболонки в нашій системі приймав значення від 11 до 11,5 мм. А різниця в 0,5 мм дає збільшення біометричної інформації на 28,52 біта.

Найчастіше порівняльний аналіз методів біометричної автентифікації проводиться на основі помилок першого і другого роду. Запропоновано виконувати порівняльний аналіз на основі критерію відносної ентропії. Порівняння проводилось за такими біометричними джерелами: зображення обличчя, райдужна оболонка ока. Виділення компонент з зображення обличчя відбувалося з використанням алгоритмів PCA, FLD і ICA. Результати порівняння наведені в таблиці 2. Виходячи з таблиці, можна зробити висновок про те, що метод розпізнавання на основі райдужної оболонки ока має більше біометричної інформації і тому дозволяє більш надійно виконувати автентифікацію особи.

Таким чином, результатом цього розділу є розроблена ентропійна модель райдужної оболонки ока, в ході використання якої можна оцінити кількість біометричної інформації, яка міститься в райдужці. Проблемним питанням було: як визначити розподіл біометричних характеристик для населення. Ми використовували типовий підхід: взяли нашу базу даних за адекватне представлення населення.

Запропоновано виконувати порівняльний аналіз методів біометричної автентифікації на основі критерію відносної ентропії. На основі проведеного порівняльного аналізу зроблено висновок про те, що райдужна оболонка ока містить більше біометричної інформації, ніж зображення обличчя. А це означає, що набір характеристик, який використовується в системі розпізнавання за райдужкою, містить більше розрізнювальної інформації, що призводить у підсумку до зниження помилок першого і другого роду. Зроблено висновок про те, що використання відносної ентропії як критерію порівняльного аналізу робить можливим не тільки порівняння

біометричних ознак між собою, але і з персональним ідентифікаційним номером (ПІН), паролем та іншими методами автентифікації

Таблиця 2 – Порівняльний аналіз методів розпізнавання за обличчям та райдужкою

Алгоритм	Біометрична інформація (біти)	
	Обличчя	Райдужка
PCA	45	278
ICA	39	288
FLD	37	

У третьому розділі запропоновано математичні моделі та методи оцінки захищеності від НСД з використанням механізмів багатофакторної автентифікації. Наводиться узагальнена модель загроз та обґрунтовуються критерії та показники оцінки захищеності ІТС (інформаційно - телекомунікаційна система) від НСД. Як основні показники захисту від НСД запропоновано такі:

1. $P_{нсд}$ (n) – ймовірність НСД у n спробах, де n – кількість спроб отримати НСД;
2. Безпечний час – $t_б$;
3. $\Delta T = T_д$ – допустимий час НСД;
4. n – кількість спроб, які можливо здійснити.

Попередній аналіз використання схем багатофакторної автентифікації показав, що в ході їх побудови можуть використовуватися механізми з послідовним, паралельним або комбінованим з'єднанням елементів, які реалізують фактори автентифікації. Розглянемо спочатку комбіновані схеми багатофакторної автентифікації із паралельно-послідовним з'єднанням елементів, коли, наприклад, можливе використання декількох факторів – паролів, біометричних ознак, ключів тощо. Така схема багатофакторної автентифікації зображена на рис. 3.

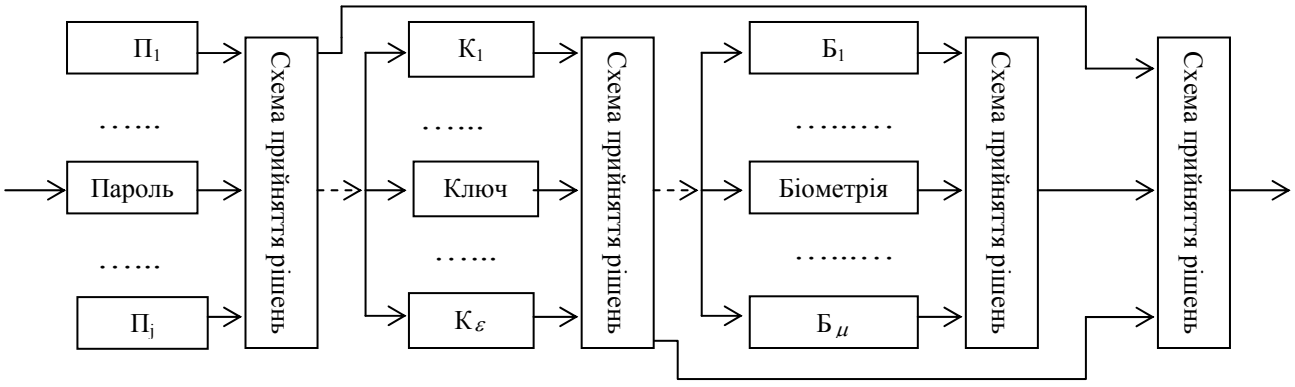

Рисунок 3 – Комбінована схема багатофакторної автентифікації

Імовірність НСД для механізму згідно з рис. 3 визначатимемо за формулою:

$$P_{НСД} = (1 - \prod_{i=1}^{j} P_i^n)(1 - \prod_{\partial=1}^{\varepsilon} P^к{}_{\partial})(1 - \prod_{l=1}^{\mu} P^б{}_l), \quad (8)$$

де $P^п$ – імовірність правильної роботи механізму паролювання, $P^к$ – імовірність правильного застосування механізму ключа, $P^б$ – імовірність правильного застосування механізму біометричних даних.

Імовірність безвідмовної (правильної) роботи механізму (рис. 3) визначатимемо за формулою:

$$P_{зах} = \prod_{i=1}^{j} P_i^n \cdot \prod_{j=1}^{\varepsilon} P^{к}{}_j \cdot \prod_{l=1}^{\mu} P^{б}{}_l \,. \tag{9}$$

У випадку використання в багатофакторному механізмі автентифікації двох факторів, механізм (рис.3) може бути поданий згідно з рис. 4, а також можливі такі комбінації: пароль(і) та ключ(і), пароль(і) та біометрична ознака(и), ключ(і) та біометрична ознака(и). В табл. 3 наведено часткові випадки моделей оцінки для трьох варіантів двофакторного механізму. В першому рядку наведено значення, які відповідають моделі, наведеній на рис. 4.

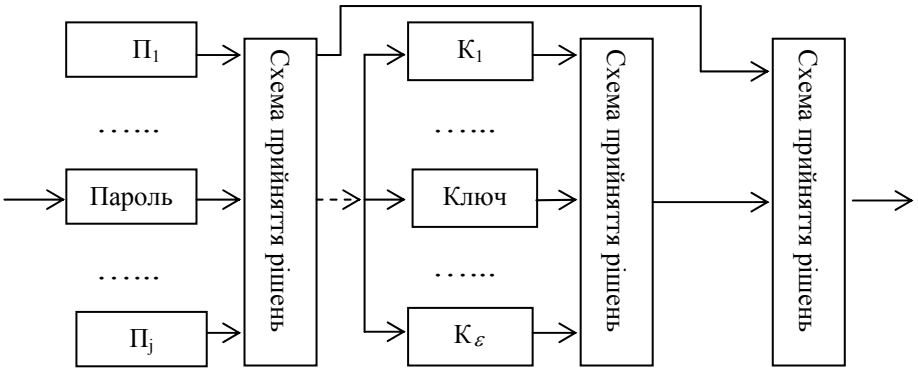

Рисунок 4 – Комбінована схема багатофакторної автентифікації «пароль та ключ»

Таблиця 3 – Співвідношення для оцінки $P_{нсд}$ ($P_{зах}$) механізмів комбінованої двохфакторної автентифікації

Механізм пароль/ключ	$P_{НСД} = (1 - \prod_{i=1}^{j} P_i^n)(1 - \prod_{\partial=1}^{\varepsilon} P^{к}{}_{\partial})$	$P_{зах} = \prod_{i=1}^{j} P_i^n \prod_{\partial=1}^{\varepsilon} P^{к}{}_{\partial}$
Механізм пароль/біометрія	$P_{НСД} = (1 - \prod_{i=1}^{j} P_i^n)(1 - \prod_{l=1}^{\mu} P^{б}{}_l)$	$P_{зах} = \prod_{i=1}^{j} P_i^n \prod_{l=1}^{\mu} P^{б}{}_l$
Механізм ключ/біометрія	$P_{НСД} = (1 - \prod_{i=1}^{\varepsilon} P_i^{к})(1 - \prod_{l=1}^{\mu} P^{б}{}_l)$	$P_{зах} = \prod_{i=1}^{\varepsilon} P_i^{к} \prod_{l=1}^{\mu} P^{б}{}_l$

На практиці, по крайній мірі, на персональних робочих станціях мають застосовуватися механізми послідовного використання різних факторів. При цьому, мають застосовуватися хоча б два різні фактори автентифікації. Частковий варіант механізму на рис. 3 зображено на рис. 5.

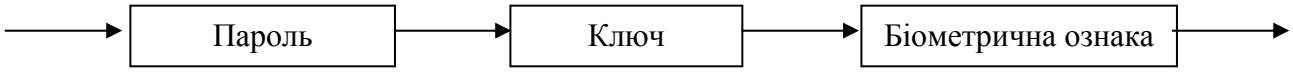

Рисунок 5 – Схема послідовного з'єднання трифакторного механізму

Ймовірність несанкціонованого доступу у послідовній структурі визначатимемо за теоремою множення ймовірностей, коли ймовірність добутку кількох незалежних

подій дорівнює добутку ймовірностей цих подій. Ймовірність НСД для рис. 5 визначатимемо згідно з формулою:

$$P_{НСД} = P^{нсд}{}_{п} \cdot P^{нсд}{}_{к} \cdot P^{нсд}{}_{б} = (1 - P_{п})(1 - P_{к})(1 - P_{б}), \quad (10)$$

де $P_п$ – імовірність правильної роботи пароля, $P_к$ – імовірність правильної роботи ключа, $P_б$ – імовірність правильної роботи біометричних даних, $P^{нсд}{}_{п}$ – імовірність підробки пароля, $P^{нсд}{}_{к}$ – імовірність підробки ключа, $P^{нсд}{}_{б}$ – імовірність підробки біометричних даних.

Далі, ймовірність безвідмовної (правильної) роботи послідовної структури для випадку, зображеному на рис. 5, визначатиметься за формулою:

$$P_{зах} = 1 - P_{нсд} = 1 - (1 - P_{п})(1 - P_{к})(1 - P_{б}). \quad (11)$$

Також практичне значення мають окремі випадки, коли застосовується один або два фактори автентифікації. У таблиці 4 наведено окремі випадки моделей оцінки для трьох варіантів двофакторного механізму автентифікації. Використовуючи наведені співвідношення, можна оцінити $P_{нсд}$ ($P_{зах}$) механізмів послідовної двофакторної автентифікації.

У табл. 3 та 4 наведено аналітичні співвідношення, які можна використовувати в ході оцінювання захищеності від НСД у разі паралельного або послідовного застосування одного фактора автентифікації.

Таблиця 4 – Співвідношення для оцінки $P_{нсд}$ ($P_{зах}$) механізмів послідовної двофакторної автентифікації

Механізм пароль/ключ	$P_{НСД} = (1 - P_{п})(1 - P_{к})$	$P_{зах} = 1 - (1 - P_{п})(1 - P_{к})$
Механізм пароль/біометрія	$P_{НСД} = (1 - P_{п})(1 - P_{б})$	$P_{зах} = 1 - (1 - P_{п})(1 - P_{б})$
Механізм ключ/біометрія	$P_{НСД} = (1 - P_{к})(1 - P_{б})$	$P_{зах} = 1 - (1 - P_{к})(1 - P_{б})$

Далі запропоновано удосконалену версію протоколу нульових знань, що базується на перетвореннях у мультиплікативній групі поля шляхом його переведення в групу точок еліптичної кривої. Розрахуємо значення стійкості I та безпечного часу t_b для алгоритмів, що базуються на перетвореннях у полях та кільцях та у групі точок еліптичної кривої (ЕКр) для таких довжин ключа: 128, 256, 512, 1024 (табл.5).

Таблиця 5 – Порівняння I та $t_б$ залежно від довжини ключа

Довжина ключа	128		256		512		1024	
	I	t_b	I	t_b	I	t_b	I	t_b
Поля та кільця	$7.1*10^{10}$	$2.3*10^{-9}$	$4.4*10^{20}$	14	$4.4*10^{20}$	14	$9.5*10^{27}$	$3.07*10^{8}$
Еліптична крива	$5.6*10^{19}$	$1.2*10^{2}$	$3.5*10^{77}$	$1.1*10^{60}$	$3.5*10^{77}$	$1.1*10^{60}$	$4.06*10^{154}$	$1.3*10^{137}$

При порівнянні цих двох алгоритмів, спостерігається збільшення часу необхідного для розкриття ключа при збереженні його довжини для алгоритму, що базується на перетвореннях у групі точок еліптичної кривої, або з іншого боку, $t_б$

залишається колишнім, а довжина ключа значно зменшується. Тому пропозицією з удосконалення протоколу автентифікації буде переклад його на ЕКр.

Для удосконалення криптографічного протоколу автентифікації за основу був взятий алгоритм електронного цифрового підпису EC-GDSA. В результаті, у протоколі нульових знань, що базується на перетвореннях у мультиплікативній групі поля необхідно зробити такі удосконалення:

- замінити випадкове число r, яке задовольняє нерівності $1 \le r \le q$, на випадкове ціле число k в інтервалі $\{1,...,n-1\}$;
- замінити доказ W на r, яке обчислюється за формулою $r = \pi(k \cdot G) mod\, n$, де G – це порядок базової точки;
- замінити ціле число d (запит), значення якого має задовольняти нерівності $0 \le d \le q$ на e, яке в свою чергу має задовольняти нерівності $1 \le e \le n$;
- замість асиметричної ключової пари (y_X, z_X), де z_X – таємний ключ, необхідно використовувати іншу ключову пару d_A, Q_A, де d_A – це секретний ключ, а відкритий ключ генерується за формулою $Q_A = d_A^{-1} \cdot G$.

Для перевірки нового алгоритму автентифікації нульових знань була розроблена програмна реалізація. Як криптографічна бібліотека була використана бібліотека Crypto + + ® Library 5.2.1. Порівняння удосконаленого та існуючого протоколів нульових знань відбувалось на основі методу аналізу ієрархій. В результаті побудови результуючого вектора значущості, отримали такі значення: існуючий протокол, заснований на перетвореннях у мультиплікативній групі поля має значущість 0,3 а удосконалений протокол – 0,7. Таким чином, кращим протоколом автентифікації є удосконалений протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕКр.

Подальші дослідження цього розділу концентрувалися на аналізі апаратно - програмних засобів автентифікації за критерієм захищеності від НСД. Основними апаратно-програмними засобами, що реалізують захищені механізми, на сьогоднішній день є смарт-картки та електронні ключі. Загальноприйняті конструкції протоколів припускають, що зловмиснику відомі вхідні і вихідні повідомлення, а будь-яка інформація про ключі йому не доступна. Але, атакуючій стороні може бути доступна і всіляка побічна інформація, яка видається криптоприладом: електромагнітне випромінювання, сигнали про помилки або про інтервали часу між виконуваними інструкціями, коливання в споживанні електроживлення та ін. Всю цю інформацію можна використовувати для аналізу і розкриття чіпів з метою доступу до секретних відомостей. Захист та контроль цілісності особистих ключів у постійному запам’ятовуючому пристрої має здійснюватися на основі пароля захисту. Особисті ключі мають контролюватися на цілісність шляхом вироблення імітовставки та захищатися шляхом зашифрування в режимі простої заміни.

Отже, у розділі запропоновано математичні моделі механізмів багатофакторної автентифікації, в ході використання яких можна оцінити ймовірності здійснення НСД на основі комбінованих та послідовних механізмів автентифікації. Розроблені математичні моделі можуть бути розповсюджені на довільний розмір простору

автентифікації і носять узагальнений характер. Важливим науковим результатом також є удосконалений протокол нульових знань, заснований на сертифікатах з використанням перетворень у групі точок ЕКр. Після проведення порівняльного аналізу і отримання результуючого вектора значущості, доведено, що удосконалений протокол має кращі властивості безпеки.

Четвертий розділ роботи присвячений методам оцінки захищеності від НСД на основі механізмів багатофакторної автентифікації. У загальній постановці сутність методів оцінки захищеності від НСД формулюється таким чином: на випадок застосування для захисту від НСД певних факторів автентифікації для кожного із факторів визначити повний перелік атак зі сторони існуючих чи потенційних криптоаналітиків (порушників) відносно аналізованого фактора, зробити їх класифікацію, вибрати критерії та показники, які дозволили б їх порівняти та вибрати такі атаки, які можуть бути реалізовані та забезпечували б досягнення максимальних значень ймовірностей НСД, тобто max $P_{нсд}$ (сформулювати пропозиції та рекомендації, в тому числі для застосування у механізмах багатофакторної автентифікації).

Як паролі можуть використовуватися паролі з m значною абеткою та довжиною пароля l_p, при чому пароль краще передавати у вигляді його геш-значення. В цьому випадку підвищується захищеність системи паролювання від компрометації фактичного значення пароля.

Сутність методу оцінки захищеності від НСД на основі парольної системи формулюємо так: якщо в ІТС(ІС, ТС, АС) для забезпечення автентифікації при доступі до інформації та ресурсів, що захищаються, використовується парольна система, для отримання доступу об'єкт (суб'єкт) повинен ввести правильно з довільного засобу (клавіатури, смарт-картки, електронного ключа тощо) конфіденційну послідовність випадкових символів – пароль. У системі автентифікації введений пароль передається певним чином до системи захисту доступу, де порівнюється з еталонною копією пароля чи його певним відображенням, наприклад геш - значенням. Також приймається модель загроз. При цьому порушник – інсайдер, що має доступ до засобу формування чи зберігання пароля, вводить пароль (пін-код) у систему. Необхідно зробити оцінку ймовірності $P_{нсд}$ та за необхідності інших показників захисту від НСД.

Ймовірність НСД $P_{нсд}$ до парольної системи визначатимемо таким чином:

$$P_{НСД} \approx \frac{n}{m^{l_n}} \qquad (12)$$

де m – основа алфавіту, l_n – довжина пароля, n – кількість спроб отримати НСД. За формулою 12 отримано значення ймовірностей НСД, коли як фактор автентифікації використовуються паролі. Оцінка ймовірностей $P_{нсд}$ виконувалась для різних значень кількості спроб n=1, 16, 2^{32}, 2^{64}, $3*10^{12}$, довжин пароля l = 4, 8, 12, 16, 32 та основи алфавіту m = 10, 16, 32, 64. Зроблено висновок про те, що для забезпечення надійної роботи механізму паролювання значення $P_{нсд}$ мають задовольняти нерівності $P_{нсд} \le 10^{-9(-6,-12,-16)}$. Встановлено:

1. При n=1, прийнятні значення $P_{нсд}$ характерні для l≥8, а m = 10, 16, 32, 64.

2. При n=16, прийнятні значення $P_{нсд}$ характерні для $l \geq 12$, а m = 10, 16, 32, 64 та для значення l = 8, коли m > 16.
3. При $n= 2^{32}$ прийнятні значення $P_{нсд}$ характерні для $l \geq 16$, а m = 10, 16, 32, 64 та для значення l = 12, коли $m \geq 32$.
4. При $n= 2^{64}$ прийнятні значення $P_{нсд}$ характерні для $l \geq 32$, а m = 10, 16, 32, 64 та для значення l = 16, коли $m \geq 64$.
5. При $n= 3*10^{12}$ прийнятні значення $P_{нсд}$ характерні для $l \geq 32$, а m = 10, 16, 32, 64 та для значення l = 16, коли $m \geq 32$, а також для значення l = 12, коли $m \geq 64$.

У загальній постановці сутність методів оцінки захищеності від НСД в ході використання асиметричних криптографічних перетворень формулюється таким чином: на випадок застосування для захисту від НСД як фактору автентифікації особистих ключів, необхідно обґрунтувати та вибрати методи криптографічних перетворень, для кожного із методів визначити та зробити класифікацію атак зі сторони існуючих чи потенційних криптоаналітиків (порушників), вибрати критерії та показники, які дозволили б їх порівняти та вибрати такі атаки, які можуть бути реалізовані та забезпечували б досягнення максимальних значень ймовірностей НСД для порушника, тобто max $P_{нсд}$, дати їм оцінку та зробити порівняльний аналіз відносно складності компрометації особистого ключа та у цілому асиметричної пари для кожного із асиметричних криптографічних перетворень, сформулювати пропозиції та рекомендації, в тому числі для застосування в механізмах багатофакторної автентифікації. При цьому фактор-носій особистого ключа розглядається окремо.

Попередній аналіз дозволив вибрати як фактори автентифікації такі асиметричні криптографічні перетворення: перетворення в кільцях (алгоритм RSA), в полі Галуа (DSA), у групі точок еліптичних кривих та в кільцях зрізаних поліномів. Вибір атаки виконувався, керуючись принципом мінімальної складності для порушника, що здійснює НСД.

Так, проаналізувавши атаки на RSA криптоперетворення, робимо висновок про те, що під час застосування квадратичного або загального решета числового поля складність факторизації RSA модуля має субекспоненційний характер. При цьому для факторизації модулів, величина яких перевищує 330–350 бітів, краще використовувати метод загального решета числового поля. Підтвердженням висловленого є попередні роботи з криптоаналізу RSA. Водночас, необхідно зазначити, що метод квадратичного решета є набагато простішим у реалізації та розумінні.

Аналіз методів дискретного логарифмування в скінченому полі Галуа F(q) підтверджує твердження про те, що методи ρ - Полларда та Поліга-Геллмана мають експоненційну складність дискретного логарифмування, а методи Адлемана, Купершмідта й решета числового поля мають субекспоненційну складність дискретного логарифмування. Виходячи з отриманих даних, можна зробити висновок про те, що найбільш простим (швидким) методом дискретного логарифмування є решето числового поля.

Виконане дослідження показує, що найшвидшим (найменш складним) алгоритмом атаки типу «повне розкриття» випадкових «неслабих» кривих над

полями $F(p)$, $F(2^m)$ і $F(p^m)$, на цей час є паралельний метод ρ-Полларда. Його складність з урахуванням ймовірності колізії P_k оцінюється як залежність вигляду:

$$I_\rho \approx \sqrt{-2n\,ln(1-P_к)}, \tag{13}$$

де n – порядок базової точки.

Відомі атаки в кільцях зрізаних поліномів можна поділити на два основних типи – грубої сили та аналітичні, які у свою чергу ґрунтуються на методах зведення в решітках. Обидва методи можуть бути використані в ході криптоаналізу, при цьому основною задачею криптоаналізу є знаходження особистого ключа.

Ймовірності НСД відносно особистого ключа для всіх названих асиметричних систем будуть малі. Їх значення можна змінювати залежно від обраних параметрів і виду асиметричного перетворення.

У загальній постановці сутність методу оцінки захищеності від НСД в ході використання біометричних ознак формулюється таким чином: на випадок застосування для захисту від НСД як фактор автентифікації тієї чи іншої біометричної ознаки, необхідно обґрунтувати та вибрати біометричні ознаки, для кожної із них вибрати критерії та показники, які дозволили б їх порівняти та вибрати такі атаки та підробку кожної біометричної ознаки, які можуть бути реалізовані та забезпечували б досягнення максимальних значень ймовірностей НСД для порушника, тобто max $Р_{нсд}$, дати біометричним ознакам оцінку та зробити порівняльний аналіз відносно складності компрометації кожної біометричної ознаки, сформулювати пропозиції та рекомендації відносно біометричних ознак, що пропонуються до використання. Як основні показники необхідно використовувати:

- $Р_{нсд}$ – ймовірність несанкціонованого доступу;
- $Р_{відм}$ – ймовірність відмови в доступі клієнту, який насправді має право на доступ;
- $Р_{зах}$ – ймовірність правильної автентифікації;
- $Р_{сер}$ – середня ймовірність помилки.

Обчислення помилок $Р_{відм}$ та $Р_{нсд}$, тобто першого і другого роду визначатимемо за формулами:

$$Р_{нсд} = \frac{n_{nд}}{n_{сд}}, \tag{14}$$

де $n_{nд}$ – загальне число доступів з помилкою (несанкціонованих), $n_{сд}$ – загальне число спроб отримати доступ.

$$Р_{відм} = \frac{n_{nв}}{n_{сд}}, \tag{15}$$

де $n_{nв}$ – загальна кількість відмов у доступі з помилкою (відмов санкціонованим користувачам).

Також відмітимо, що обчислюватимемо $Р_{зах}$ як:

$$Р_{зах} = 1 - Р_{нсд}. \tag{16}$$

Це можна пояснити тим, що $P_{зах}$ та $P_{нсд}$ складають повну групу подій.

Таким чином, для методу автентифікації на основі біометричних ознак ступінь захищеності від несанкціонованого доступу можна оцінити, використовуючи значення $P_{нсд}$ (FAR) незалежно від того, скільки факторів використовується в ході автентифікації. Але проектування системи захисту від НСД має здійснюватися з урахуванням вимог $P_{відм}$.

Важливим результатом цього розділу є розроблені методи оцінки захищеності з використанням механізмів багатофакторної автентифікації. В процесі побудови системи захисту від НСД спочатку визначається перелік факторів, які можна застосувати для здійснення багатофакторної автентифікації. Потім для кожного із факторів необхідно визначити повний перелік атак зі сторони існуючих чи потенційних криптоаналітиків та дати їм оцінки. На основі отриманих результатів формулюються пропозиції та рекомендації відносно факторів, а також обґрунтовується та вибирається протокол автентифікації.

Як криптографічне перетворення краще використовувати перетворення у групі точок еліптичної кривої у вигляді ЕЦП (електронного цифрового підпису), причому як фактор має застосовуватися особистий ключ ЕЦП, оскільки в такому випадку забезпечується експоненційна стійкість проти атак, достатня швидкодія та існують стандартизовані примітиви ЕЦП.

Отримані в четвертому розділі наукові та практичні результати підтвердили можливість реалізувати метод багатофакторної автентифікації. Залежно від вимог та моделі загроз, для захисту від НСД може бути використаною як двофакторна, так і трифакторна автентифікація.

П'ятий розділ дисертації присвячено експериментальній оцінці та аналізу захищеності від НСД з використанням механізмів багатофакторної автентифікації.

Використовуючи запропонований у дисертації метод оцінки захищеності від НСД на основі асиметричних криптоперетворень, розрахована оцінка захищеності від НСД в ході використання RSA перетворення, DSA криптоалгоритму, криптоалгоритму EC-DSA та NTRU.

Як було зазначено раніше, найкращим алгоритмом факторизації на сьогодні вважається метод загального решета числового поля та його спеціальні моделі. Метод загального решета числового поля (NSF - number field sieve) дозволяє факторизувати модуль RSA перетворення зі складністю:

$$I_{RSA} = exp\left[\delta\left(ln\, N_j\right)^{\upsilon}\left(ln\, ln\, N_j\right)^{1-\upsilon}\right], \qquad (17)$$

де $\delta = 1{,}9;\ \upsilon = 1/3$, N – розмір простору ключів.

Реальним параметром оцінки складності факторизації є безпечний час ($t_б$), тобто математичне сподівання часу здійснення НСД до інформації, що захищається із заданою ймовірністю. Далі у розділі наводяться результати розрахунків у формі таблиць значень складності криптоаналізу та безпечного часу RSA криптоалгоритму методом решета числового поля для $N = 2^{512}$, 2^{1024}, 2^{2048}, 2^{3072}, 2^{4096}, 2^{8192}, 2^{15360}, 2^{16384}. Приймається, що потужність криптосистеми $\gamma = 10^{10}, 10^{12}$ операцій за секунду. З отриманих даних зроблено висновок про те, що вже при довжині ключа RSA перетворення 1024 біта, кількість часу, необхідного для розкриття криптоалгоритму

$10^6 – 10^8$ років. Таким чином, алгоритм RSA захищений від атаки «повне розкриття» вже на довжині ключа 1024 біта. Проте відзначається, що за певних умов при багатофакторній автентифікації може бути застосований і ключ довжиною 512 біт.

Аналогічно і для дискретного логарифмування в скінченому полі Галуа розроблено та застосовується решето числового поля (NFS). Воно є найбільш ефективним щодо мінімальної складності дискретного логарифмування в скінченому полі Галуа. Формула для оцінки складності дискретного логарифмування в скінченому полі Галуа методом решета числового поля виглядає таким чином:

$$I_{DSA} = exp\left[\delta\left(ln\, N_j\right)^{\upsilon}\left(ln\, ln\, N_j\right)^{1-\upsilon}\right], \qquad (18)$$

де приймемо, що $\delta = 1{,}96;\ \upsilon = 1/3$.

Розрахунок значень складності криптоаналізу та безпечного часу DSA криптоалгоритму методом загального решета числового поля виконувався для N = 2^{512}, 2^{1024} , 2^{2048}, 2^{3072}, 2^{4096}, 2^{8192}, 2^{15360}, 2^{16384} . Приймалося, що потужність криптосистеми γ = 10^{10} , 10^{12} операцій за секунду. З отриманих даних зроблено висновок про те, що вже при довжині ключа DSA перетворення 1024 біта кількість часу, необхідного для розкриття криптоалгоритму, складає 10^7 - 10^9 років. Таким чином, алгоритм DSA захищений від атаки «повне розкриття» вже на довжині ключа 1024 біта, але за певних умов при багатофакторній автентифікації може бути застосований і ключ довжиною 512 біт.

Здійснення атаки «повне розкриття» у групі точок еліптичної кривої безпосередньо пов’язане із розв’язанням задачі дискретного логарифмування у групі точок еліптичної кривої. Як зазначалось раніше, найкращим алгоритмом атаки типу «повне розкриття» випадкових «неслабих» кривих над полями $F(p)$, $F(2^m)$ і $F(p^m)$ на сьогодні є паралельний метод ρ-Полларда. Його складність з урахуванням імовірності колізії та того, що $I^2 >> I$, можна розрахувати за формулою 13. Результати розрахунків значень складності криптоаналізу методом ρ - Полларда та безпечного часу криптоалгоритму EC-DSA для n = 2^{160}, 2^{192}, 2^{256}, 2^{341}, 2^{509}, 2^{571} та для різних значень $P_к$=0,5; 0.99 наведено в таблицях розділу. Для криптоалгоритму EC-DSA приймалося, що потужність криптосистеми γ=10^{10} /20 або 10^{12} /20 операцій за секунду. Із отриманих даних зроблено висновок про те, що вже при порядку базової точки 2^{160} кількість часу, необхідного для розкриття криптоалгоритму 10^5 - 10^8 років. Таким чином, алгоритм на еліптичній кривій захищений від атаки «повне розкриття» вже на довжині ключа 160 біт.

Порівняно з алгоритмами DSA та RSA бачимо збільшення часу, необхідного для розкриття ключа для алгоритму, що базується на перетвореннях у групі точок еліптичної кривої, або з іншого боку, $t_б$ залишається колишнім, а довжина ключа значно зменшується.

Встановлено, що здійснення атаки типу повне розкриття у фактор-кільці зрізаних поліномів характеризується експоненційним рівнем складності. Також криптосистема NTRU характеризується суттєво підвищеною швидкодією у порівнянні з іншими криптоперетвореннями, які розглянуті вище. Але це

відноситься тільки до направленого шифрування. Відносно ЕЦП у кільцях зрізаних поліномів суттєвих досягнень щодо стійкості і швидкодії немає.

У дисертаційній роботі отримано оцінки складності криптоаналізу NTRU НШ (направленого шифрування) з використанням атаки «груба сила» та «зустріч посередині». Складність реалізації атаки «груба сила» була визначена за формулою:

$$T = C_N^{d_f} \; C_{N-d_f}^{d_f-1}, \tag{19}$$

де N – розмір кільця R (максимальний степінь поліномів кільця), d_f – кількість одиничних коефіцієнтів ключового багаточлена f(x), d_f -1 – кількість коефіцієнтів ключового багаточлена f(x), які дорівнюють –1. Для розрахунків складності криптоаналізу використано загальні параметри NTRU, що рекомендуються до застосування. В результаті проведених розрахунків отримано, що при N = 167 і d_f = 61 – значення $T = 6.5 * 10^{76}$, при N = 251 і d_f = 50 – значення $T = 3.3 * 10^{100}$, при N = 503 і d_f = 216 – значення $T = 1.4 * 10^{216}$.

Із отриманих оцінок зроблено висновок про те, що атака «груба сила» є складною і практично не здійсненною відносно направленого шифру на NTRU.

Для визначення складності реалізації атаки «зустріч посередині» використано таку формулу:

$$I = C_{N/2}^{d/2}. \tag{20}$$

З розрахунків отримаємо для NTRU з параметрами N = 167, d = 61, простір ключів має розмір ≈ $2.6 * 10^{46}$, а при N = 503, d = 216, простір ключів має розмір ≈ $6.2 * 10^{147}$.

Вищенаведене дозволяє зробити висновок, що для того, щоб гарантувати криптографічну стійкість з рівнем 2^x, необхідно використовувати NTRU з розміром простору ключів 2^{2x}.

Подальша робота в цьому розділі присвячена важливій з практичної точки зору задачі – отримання оцінок ймовірностей НСД у схемах багатофакторної автентифікації. Ці оцінки ґрунтуються на розрахунках та формулах, отриманих у попередніх розділах.

Ймовірність НСД до ключа за рік визначалась за такою формулою:

$$P_{НСД}^{кл} = \frac{k \cdot \gamma}{N}, \tag{21}$$

де N – кількість операцій (складність криптоаналізу), $k \approx 3{,}15 \cdot 10^7$ (с), кількість секунд у році, γ – кількість операцій за секунду, виконуваних системою криптоаналітика для заданого алгоритму. Цю формулу можна отримати з формули $t_б$, прийнявши $t_б$=1. Ймовірності НСД до ключа матимуть дуже малі значення. Вони можуть змінюватися залежно від обраних криптоперетворень. Використовувались такі значення ймовірностей НСД до ключа: $P^к_{нсд} = 10^{-6}, 10^{-19}, 10^{-32}$. Ймовірності НСД щодо парольної та щодо біометричної системи були взяті з розрахунків попередніх розділів. За основу для розрахунків була взята математична модель, зображена на рисунку 5, а також співвідношення для оцінки $P_{нсд}$ з таблиці 4. Результати

розрахунків $P_{нсд}$ у механізмах багатофакторної автентифікації наведені в численних таблицях розділу. Приклад двох з таких таблиць наведений нижче. Так, у таблиці 6 наведено значення $P_{нсд}$ для випадку послідовного двофакторного механізму «пароль+ключ». Відповідно, в таблиці 7 наведено значення $P_{нсд}$ для випадку послідовного трифакторного механізму «ключ+біометрія+пароль», коли $P_{нсд}$ для парольної системи = $3{,}7*10^{-9}$.

Таблиця 6 – Значення $P_{нсд}$ для системи «пароль+ключ»

$P^{п}_{нсд}$ \ $P^{к}_{нсд}$	10^{-6}	10^{-19}	10^{-32}
$4*10^{-3}$	$4*10^{-9}$	$4*10^{-22}$	$4*10^{-35}$
$3.7*10^{-9}$	$3{,}7*10^{-15}$	$3{,}7*10^{-28}$	$3{,}7*10^{-41}$
$1.8*10^{-13}$	$1{,}8*10^{-19}$	$1{,}8*10^{-32}$	$1{,}8*10^{-45}$
$5.4*10^{-20}$	$5{,}4*10^{-26}$	$5{,}4*10^{-39}$	$5{,}4*10^{-52}$
$2.9*10^{-39}$	$2{,}9*10^{-45}$	$2{,}9*10^{-58}$	$2{,}9*10^{-71}$
$1.6*10^{-58}$	$1{,}6*10^{-64}$	$1{,}6*10^{-77}$	$1{,}6*10^{-90}$

Таблиця 7 – Значення $P_{нсд}$ для системи «ключ+біометрія+пароль» при $P^{п}_{нсд}= 3{,}7*10^{-9}$

$P^{к}_{нсд}$ \ $P^{б}_{нсд}$	10^{-4}	10^{-6}	10^{-3}
10^{-6}	$3{,}7*10^{-19}$	$3{,}7*10^{-21}$	$3{,}7*10^{-18}$
10^{-19}	$3{,}7*10^{-32}$	$3{,}7*10^{-34}$	$3{,}7*10^{-31}$
10^{-32}	$3{,}7*10^{-45}$	$3{,}7*10^{-47}$	$3{,}7*10^{-44}$

З отриманих нами даних можна зробити висновок про те, що найбільш захищеною схемою багатофакторної автентифікації є схема, в якій використовуються три фактори автентифікації: наприклад, біометрія, ключ та пароль. Але використання трифакторних схем одночасно є і найбільш складним варіантом, як в обчислювальному, так і в організаційно-технічному сенсі.

Основною перевагою трифакторної автентифікації є те, що при компрометації навіть двох факторів забезпечується достатній рівень захищеності від НСД. Також, хоча під час досліджень ми вважали усі фактори рівнозначними, насправді фактори, які пов’язані з асиметричними криптоперетвореннями, а також в ході використання електронних носіїв особистого ключа є більш надійними. Оцінка та дослідження механізмів автентифікації здійснювались для три-, дво- та однофакторної автентифікації. Водночас усі отримані співвідношення та результати можна розповсюдити і на механізми з більшою кількістю факторів. На наш погляд це можна робити в багаторівневих корпоративних та глобальних інформаційно-комунікаційних системах.

Таким чином, основним результатом цього розділу є отримані значення ймовірностей НСД для різних варіантів багатофакторної автентифікації, що дозволяє обрати схему багатофакторної автентифікації, яка має мінімальне значення ймовірності НСД. У цілому запропоновані механізми часткових оцінок різних варіантів багатофакторної автентифікації свідчать як про можливість їх реалізації з точки зору складності, так і застосування за різних вимог та параметрів механізмів багатофакторної автентифікації.

Висновки містять основні наукові та практичні результати, отримані під час дисертаційних досліджень.

У **додатках** наведено доведення формул $P_{нсд}$ та $P_{зах}$ для комбінованої схеми багатофакторної автентифікації та послідовного з'єднання елементів, порівняльний аналіз існуючого протоколу нульових знань, описаного в стандарті ДСТУ ISO/IEC 9798-5 та удосконаленої його версії на основі методу аналізу ієрархій, класифікація та визначення смарт-карток, життєвий цикл смарт-картки та рекомендації щодо впровадження системи смарт-карток в Україні, а також акти впровадження отриманих результатів.

ВИСНОВКИ

В результаті виконаних досліджень у рамках дисертаційної роботи розв'язано важливу наукову-технічну задачу з розробки математичних моделей та методів оцінки захищеності від НСД інформації та ресурсів з використанням механізмів багатофакторної автентифікації, що дозволяє мінімізувати ймовірності НСД щодо інформації та ресурсів.

Висновки, сформульовані в роботі, полягають в наступному.

1. Розроблено та обґрунтовано нові моделі оцінки захищеності від НСД інформації та ресурсів з використанням механізмів багатофакторної автентифікації, в ході використання яких можна оцінити ймовірності здійснення НСД та ймовірності безвідмовної роботи на основі комбінованих та послідовних механізмів автентифікації. З урахуванням вимог відносно оперативності автентифікації рекомендується застосовувати не більше як трифакторну автентифікацію. Розроблені математичні моделі можуть бути розповсюджені на довільний розмір простору автентифікації і носять узагальнений характер.

2. Набув подальшого розвитку метод автентифікації, що ґрунтується на перетвореннях у скінченому полі, який відрізняється від відомого використанням механізму, що розглянутий вище, у групі точок еліптичної кривої. Це дозволило досягти експоненційного рівня складності реалізації атаки «повне розкриття», а також зменшити довжину ключа при збереженні показника безпечного часу.

3. Запропоновано нові методи оцінки захищеності від НСД з використанням механізмів багатофакторної автентифікації, які полягають у тому, що в ході синтезу системи захисту від НСД визначається перелік факторів, які можна застосувати для здійснення, наприклад, трифакторної автентифікації. Далі для кожного із факторів визначається повний перелік атак зі сторони існуючих чи потенційних криптоаналітиків (порушників), формулюються критерії та показники, які дозволили б їх порівняти та вибираються такі атаки, які можуть бути реалізовані та забезпечували б досягнення максимальних значень ймовірностей НСД, тобто max $P_{нсд}$, потім формулюються пропозиції та рекомендації, в тому числі для застосування у механізмах багатофакторної автентифікації, а також обґрунтовується та вибирається протокол автентифікації. Ті механізми вважаються більш захищеними, які мають значення $P_{нсд}$ найменше. Розроблений метод дозволяє оцінити ймовірності НСД як в ході використання кожного фактора автентифікації окремо, так і в схемах багатофакторної автентифікації взагалі.

4. Запропоновано ентропійну модель райдужної оболонки ока, яка полягає у визначенні кількості біометричної інформації райдужної оболонки ока та дозволяє обчислити кількість інформації, яка міститься в райдужці та порівняти її не тільки з іншими біометричними ознаками, але і з ПІН кодом, паролем та іншими методами автентифікації. Встановлено, що зображення райдужки містить більше біометричної інформації, ніж зображення обличчя і тому дозволяє більш надійно автентифікувати особу.

Достовірність отриманих наукових результатів підтверджується математичною коректністю введених моделей; несуперечливістю з відомими результатами теорії надійності, теорії автентифікації, теорії асиметричних криптоперетворень, несуперечливістю з результатами, отриманими в окремих теоріях та їх збігом з відомими чи отриманими експериментально.

Практична значущість отриманих результатів полягає у тому, що:

1. Розраховано кількість біометричної інформації, що міститься в райдужній оболонці ока і зроблено її порівняльний аналіз із кількістю біометричної інформації, яка міститься в обличчі. Показано, що зображення райдужної оболонки ока має більшу кількість біометричної інформації. Так, кількість біометричної інформації для райдужної оболонки ока складає 278–288 біт, в той час, як для зображення обличчя – 37–45 біт, залежно від обраного алгоритму. З отриманих значень робимо висновок про те, що розпізнавання на основі райдужної оболонки ока буде більш надійним.

2. Проведено порівняльний аналіз методів біометричної автентифікації на основі помилок першого, другого роду та коефіцієнта рівної ймовірності помилок та надано рекомендації стосовно їх застосування в протоколах багатофакторної автентифікації. Найкращим методом біометричної автентифікації, який рекомендовано застосовувати в протоколах багатофакторної автентифікації є автентифікація на основі райдужної оболонки ока. Коефіцієнт рівної ймовірності помилок для райдужки складає $2{,}1*10^{-3}$, а помилка другого роду (або $P_{нсд}$) – $1*10^{-6}$. Як додаткові параметри можна використовувати відбиток пальця або геометричну форму кисті руки.

3. Проведено порівняльний аналіз удосконаленого протоколу нульових знань, заснованого на використанні перетворень у групі точок еліптичної кривої та існуючої версії, яка заснована на перетвореннях у мультиплікативній групі поля на основі методу аналізу ієрархій. Встановлено, що удосконалена версія має кращі властивості безпеки. На основі побудови результуючого вектора значущості отримано такі значення: значущість удосконаленої версії – 0,7, а існуючої – 0,3. Таким чином, кращим протоколом, який рекомендовано до застосування, визнано удосконалений протокол нульових знань, заснований на сертифікатах з використанням перетворень у групі точок еліптичної кривої.

4. Розроблено комплекси програмного забезпечення (програмні моделі), які реалізують обчислення біометричної інформації райдужної оболонки ока для алгоритмів PCA та ICA та програмне моделювання удосконаленої версії протоколу нульових знань.

5. Отримано значення ймовірностей НСД для парольної системи автентифікації, для системи автентифікації на основі асиметричних пар ключів та

для біометричних систем автентифікації, а також значення ймовірностей НСД для дво- та трифакторних систем автентифікації. Найбільш захищеним механізмом багатофакторної автентифікації є механізм, у якому використовуються три фактори автентифікації, наприклад: біометрія, ключ та пароль. Імовірність $P_{нсд}$ при цьому може мати значення $1{,}6*10^{-93}$. Крім того, хоча під час досліджень ми вважали усі фактори рівнозначними, насправді фактори, що пов'язані з асиметричними криптоперетвореннями, а також в ході використання електронних носіїв особистого ключа, є швидше всього більш надійними.

В цілому отримані наукові та практичні результати підтвердили можливість реалізації механізмів багатофакторної автентифікації. Залежно від вимог та моделі загроз для захисту від НСД може використовуватися як двофакторна, так і трифакторна автентифікація. Основною перевагою трифакторної автентифікації є те, що при компрометації навіть двох факторів забезпечується достатній рівень захищеності від НСД. Водночас механізм трифакторної автентифікації одночасно є і найбільш складним як в обчислювальному, так і в організаційно-технічному сенсі. Розроблені математичні моделі багатофакторної автентифікації можуть бути розповсюджені на довільний розмір простору автентифікації і носять узагальнений характер.

Результати досліджень використано в ході виконання низки НДР, у навчальному процесі з дисципліни «Прикладна криптологія», у виданому підручнику «Прикладна криптологія. Теорія. Практика. Застосування» авторів І. Д. Горбенко, Ю. І. Горбенко, впроваджені в діяльність приватного акціонерного товариства «Інститут інформаційних технологій».

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Горбенко Ю. И. Модели и методы оценки защищенности механизмов многофакторной аутентификации / Ю. И. Горбенко, И. В. Олешко // Восточно-европейский журнал передовых технологий: научный журнал. – 2012. – № 6/2(66). – С. 4 – 10.

2. Горбенко И. Д. Метод оценки относительной энтропии и сравнительный анализ источников биометрической информации / И. Д. Горбенко, И. В. Олешко // Прикладная радиоэлектроника: научно-техн. журнал. – 2012. – Том 11, № 2. – С. 255 – 261.

3. Олешко І. В Удосконалення протоколу нульових знань, заснованого на дискретних логарифмах / І. В. Олешко // Прикладная радиоэлектроника: Научно-техн. журнал. – 2013. – № 2. – С. 363 – 372.

4. Горбенко И. Д. Методы биометрической аутентификации для использования в паспортной системе / И. Д. Горбенко, И. В. Олешко // Прикладная радиоэлектроника: научно-техн. журнал. – 2011. – Том 10, № 2. – С. 255 – 258.

5. Олешко И. В. Сравнительный анализ протоколов строгой аутентификации [Текст] / И. В. Олешко, И. Д. Горбенко // Радиотехника. – 2012. – №3 – С. 198 – 210.

6. Олешко І. В. Порівняльний аналіз методів біометричної автентифікації на основі критерію відносної ентропії / І. В. Олешко // Вісник національного університету "Львівська політехніка". – 2012. – С. 170 – 175.

7. Олешко І. В. Порівняльний аналіз джерел біометричної інформації та метод оцінки їх ентропії / І. В. Олешко // XI міжнародна науково-технічна конференція Авіа-2013: Зб. матеріалів форума, Київ, 21- 23 трав. 2013р. – Т.1. – К.: НАУ, 2013. – С. 2.21 – 2.24.

8. Олешко И. В. Оценка энтропии и использование биометрических данных для аутентификации / И. В. Олешко // Компьютерное моделирование в наукоемких технологиях (КМНТ-2012): сб. материалов форума, Харьков, 24-27 апр. 2012 г. – Х.: ХНУ, 2012. – С. 322 – 325.

9. Олешко И. В. Усовершенствование протокола аутентификации с нулевым разглашением / И. В. Олешко // Безопасность информации в информационно-телекоммуникационных системах: материалы XVI международной научно-практической конференции, Киев, 21-24 мая 2013г. – Киев: Госспецсвязь, 2013. – С. 42 – 43.

10. Олешко І. В. Методи біометричної автентифікації для застосування в паспортній системі / І. В. Олешко // Наука и социальные проблемы общества: информатизация и информационные технологи: мат. VI-ї міжнародної науково-практичної конференції, Харків, 24-25 трав. 2011р. – Х.: ХНУРЕ, 2011. – С. 254–255.

11. Олешко І. В. Порівняльний аналіз методів біометричної автентифікації на основі критерію відносної ентропії / І.В. Олешко // Захист інформації і безпека інформаційних систем: мат. І-ї міжнародної науково-технічної конференції, Львів, 31 трав.-1черв. 2012р. – Л.: Національний університет “Львівська політехніка”, 2012. – С. 98 – 99.

12. Олешко И. В. Использование относительной энтропии для оценки биометрической информации / И. В. Олешко // Безопасность информации в информационно-телекоммуникационных системах: материалы XV юбилейной международной научно-практической конференции, Киев, 22-25 мая 2012г. – Киев: Госспецсвязь, 2012. – С. 45 – 47.

13. Олешко І. В. Порівняльний аналіз методів біометричної автентифікації для використання в електронних паспортах / І. В. Олешко // Радиоэлектроника и молодежь в XXI веке: мат. 15-го ювілейного міжнародного молодіжного форуму, Харків, 18-20 трав. 2011. – Харків: ХНУРЕ, 2011. – С. 177 – 178.

14. Олешко И. В. Сравнительный анализ методов аутентификации по отпечатку пальца / И. В. Олешко // Прикладная радиоэлектроника. Состояние и перспективы развития МРФ-2011: мат. IV-го международного радиоэлектронного форума, Харьков, 19-22 октяб. 2011г. – Харьков: ХНУРЭ, 2011. – С. 335 – 338.

АНОТАЦІЯ

Олешко І. В. Моделі та методи оцінки захищеності механізмів багатофакторної автентифікації від несанкціонованого доступу. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації. – Харківський національний університет радіоелектроніки МОН України, Харків, 2014.

Мета дисертаційного дослідження – розробка математичних моделей та методів оцінки захищеності від НСД інформації та ресурсів з використанням механізмів багатофакторної автентифікації та порівняльний аналіз механізмів багатофакторної автентифікації, що дозволяє мінімізувати ймовірності НСД щодо інформації та ресурсів.

Запропоновано математичні моделі оцінки захищеності від НСД інформації та ресурсів з використанням механізмів багатофакторної автентифікації, які базуються на обчисленні ймовірностей НСД та безвідмовної роботи механізмів, що дозволяє оцінити ймовірності НСД у схемах багатофакторної автентифікації.

Запропоновано методи оцінки захищеності від НСД з використанням механізмів багатофакторної автентифікації, які базуються на визначенні повного переліку атак відносно аналізованого фактора, їх класифікації, аналізу критеріїв та показників, які дозволяють їх порівняти та вибору таких атак, які можуть бути реалізовані та забезпечували б досягнення максимальних значень складностей криптоаналізу, що дозволяє оцінити ймовірності НСД як під час використання кожного фактора окремо, так і в схемах багатофакторної автентифікації взагалі.

Запропоновано ентропійну модель райдужної оболонки ока, яка базується на визначенні кількості інформації, яка міститься в райдужній оболонці, що дозволяє обчислити кількість біометричної інформації райдужки та порівнювати не тільки біометричні ознаки між собою, але і з ПІН кодом, паролем та іншими методами автентифікації в ході використання їх ентропійних оцінок.

Удосконалено метод автентифікації, який описано в стандарті ДСТУ ISO/IEC 9798-5, що відрізняється від існуючого тим, що замість перетворень у мультиплікативній групі поля використовуються перетворення у групі точок еліптичної кривої, що дозволяє досягти експоненційного рівня складності здійснення атаки «повне розкриття», а також зменшити довжини ключа при збереженні показника безпечного часу.

Ключові слова: несанкціонований доступ, багатофакторна автентифікація, ентропійна модель, безпечний час, протокол нульових знань, механізм паролювання, біометрична ознака.

АННОТАЦИЯ

Олешко И. В. Модели и методы оценки защищенности механизмов многофакторной аутентификации от несанкционированного доступа. - На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 - системы защиты информации. - Харьковский национальный университет радиоэлектроники МОН Украины, Харьков, 2014 .

Цель диссертационного исследования – разработка математических моделей и методов оценки защищенности от НСД информации и ресурсов с использованием механизмов многофакторной аутентификации и сравнительный анализ механизмов многофакторной аутентификации, что позволяет минимизировать вероятности НСД к информации и ресурсам.

Предложены математические модели оценки защищенности от НСД информации и ресурсов с использованием механизмов многофакторной аутентификации, основанные на вычислении вероятностей НСД и безотказной работы механизмов, позволяющие оценить вероятности НСД в схемах многофакторной аутентификации.

Предложены методы оценки защищенности от НСД с использованием механизмов многофакторной аутентификации, основанные на определении полного перечня атак в отношении рассматриваемого фактора, их классификации, анализе критериев и показателей, позволяющих их сравнить и выбора таких атак, которые могут быть реализованы и обеспечивали бы достижение максимальных значений сложностей криптоанализа, что позволяет оценить вероятности НСД как при использовании каждого фактора в отдельности, так и в схемах многофакторной аутентификации в общем.

Предложена энтропийная модель радужной оболочки глаза, которая базируется на определении количества информации, содержащейся в радужной оболочке, которая позволяет вычислить количество биометрической информации радужки и сравнивать не только биометрические признаки между собой, но и с ПИНом, паролем и другими методами аутентификации при использовании их энтропийных оценок.

Усовершенствован метод аутентификации, описанный в стандарте ISO/IEC 9798-5, отличающийся от существующего тем, что вместо преобразований в мультипликативной группе поля используются преобразования в группе точек эллиптической кривой, что позволяет достичь экспоненциального уровня сложности осуществления атаки «полное раскрытие», а также уменьшить длины ключа при сохранении показателя безопасного времени.

Ключевые слова: несанкционированный доступ, многофакторная аутентификация, энтропийная модель, безопасное время, протокол нулевых знаний, механизм паролирования, биометрический признак.

ABSTRACT

Oleshko I. V. Models and methods for assessing security of multi-factor authentication mechanisms from unauthorized access. – The manuscript.

Thesis for Ph.D. science degree by specialty 05.13.21 – information security systems. – Kharkiv National University of Radioelectronics of the MES of Ukraine, Kharkiv, 2014.

The dissertation is devoted to development of mathematical models and methods for assessing information and resources security from unauthorized access using multi-factor authentication (MFA) mechanisms and comparative analysis of MFA mechanisms to minimize the probability of unauthorized access to information and resources.

This paper describes mathematical models for assessing information and resources security from unauthorized access using MFA mechanisms based on the calculation of unauthorized access probabilities and uptime probabilities to estimate unauthorized access probabilities for multi-factor authentication schemes.

Also it describes methods for assessing security from unauthorized access using MFA mechanisms based on attacks complete list determining against this factor, attacks classification, analysis of criteria and indicators compare and choose from such attacks, which can be implemented and would ensure the achievement of the maximum complexity values of cryptanalysis. These methods allow to estimate unauthorized access probabilities as using each factor separately and in a MFA schemes in general.

Here we propose the iris entropy model based on the quantity of information contained in the iris, which allows to calculate the amount of iris biometric information and compare not only the biometric features among themselves but also with the PIN, password and other authentication means by using their entropy estimates.

Also we improve ISO/IEC 9798-5 authentication method by changing transformations in the multiplicative group to the group of points of an elliptic curve to achive the exponential complexity for the "full disclosure" attack, as well as reduce key length while preserving the safety time.

Keywords: unauthorized access, multifactor authentication, entropy model, safe time, zero-knowledge protocol, password protecting mechanism, biometric feature.

Підп. до друку 28.02.2014. Формат 60х84 1/16. Спосіб друку – ризографія.
Умов.друк.арк. 1,7. Облік. вид.арк. 1,5. Тираж 100 прим.
Ціна договірна Зам № 2-183.

ХНУРЕ. Україна. 61166, Харків, просп. Леніна, 14

Віддруковано в навчально-науковому
видавничо-поліграфічному центрі ХНУРЕ
61166, Харків, просп. Леніна, 14