УДК 519.81 DOI: 10.30748/zhups.2021.67.09

І.Є. Ряполов, Я.І. Кметюк, М.С. Дубинець

Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків

АНАЛІЗ МЕТОДІВ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ НА ОСНОВІ БІОТЕХНОЛОГІЙ

В сучасних умовах проблема інформаційної безпеки системи управління набуває особливого значення в умовах широкого застосування автоматизованих інформаційних систем. Забезпечення інформаційної безпеки повинно носити системний характер. В результаті проведеного дослідження встановлено, що існує велика кількість інструментів забезпечення інформаційної безпеки, які мають недоліки, пов'язані із захистом та дискримінацією, можливістю підробки паролю, невиконанням інструкцій по створенню безпечного пароля користувачем, існуванням і наявністю у вільному доступі спеціалізованих додатків для підбору і злому паролів. Людський фактор являється основним недоліком даних систем. Єдиного підходу щодо підвищення інформаційної безпеки інформаційно-телекомунікаційної системи Повітряних Сил не існує. Проведено аналіз застосування біотехнологій ідентифікації доступу з застосуванням стеганографічного методу захисту інформації. Метод підвищення інформаційної безпеки інформаційно-телекомунікаційної системи, в основі якого запропоновано використання процедури розпізнавання особи за райдужною оболонкою та реакцією очного яблука людини на подразники. Запропонований підхід щодо захисту інформації з використанням біометричних методів ідентифікації користувачів зменшить вплив "людського" фактору, що підвищить ефективність процедури ідентифікації та автентифікації.

Ключові слова: *біотехнології, ідентифікація, аутентифікація, верифікація, системи доступу, шаблон, зіставлення, сховище даних.*

Вступ

Постановка проблеми. Сучасний етап розвитку інформаційно-телекомунікаційних систем (ІТС) характеризується суттєвими, з одного боку, широкими впровадженнями інформаційних технологій в соціальну, політичну, соціально-політичну та економічну сфери діяльності, а з іншого – призводить до ведення інформаційних війн з метою створення нестабільності різних суспільних факторів. У протидії інформаційним війнам слід приділяти велику увагу захисту державним інформаційним ресурсам. Адже загрози інформаційній безпеці держави відіграють головну роль в системі захисту ІТС [1]. Досвід локальних конфліктів останніх десятиліть, в тому числі на території Донецької та Луганської областей України, свідчить про динамічність та складність обстановки в ході підготовки та ведення бойових дій. Це обумовлює підвищення значення боротьби для досягнення успіху не лише в окремих операціях збройних сил, але й у війні в цілому [1–2]. Досягти ефективності результату бойових дій можливо тільки шляхом створення ефективної системи управління, яка повинна функціонувати в єдиному інфокомунікаційному просторі в реальному масштабі часі, забезпечувати обробку інформації, виробку управляючих дій. При цьому проблема інформаційної безпеки системи управління набуває особливого значення в сучасних умовах широкого застосування ІТС. У зв'язку із великою кількістю кібернетичних та інформаційних атак з боку противника зростає необхідність в захисті інформаційних ресурсів та об'єктів управління. Аналіз показав, що одним з можливих рішень задачі підвищення безпеки інформаційних систем є створення біометричної системи ідентифікації доступу з застосуванням стеганографічного методу захисту інформації. Методи стеганографії дозволяють не тільки приховано передавати дані, але й успішно вирішувати завдання завадостійкої автентифікації, захисту інформації від несанкціонованого копіювання, відстеження поширення інформації мережами зв'язку, пошуку інформації в мультимедійних базах даних.

У зв'язку з цим виникає актуальна задача щодо розробки підходів по підвищенню інформаційної безпеки інформаційно-телекомунікаційної системи Повітряних Сил з врахуванням розмежувального доступу до інформаційних ресурсів.

Аналіз останніх досліджень і публікацій. На даний момент прийняті на озброєння та впроваджені системи обміну даними, які використовують саме криптографічний підхід щодо захисту інформації.

Так для поліпшення оперативно-технічних характеристик в системі захисту інформації комплексу засобів автоматизації використовується комбінація методів ідентифікації по динаміці підпису, спектру мови і персонального коду, записаного в електро-

нному ключі типу “Touch memory”, що не є досить надійним підходом. Проведений аналіз показав, що методи, які забезпечують ідентифікацію доступу до автоматизованих та інформаційних систем, не враховують напрямок, заснований на біотехнологіях. Тому його впровадження, як додаткового механізму, дозволяє збільшити ступінь захищеності від несанкціонованого доступу та здійснення кібернетичних атак [6–10].

Серед найважливіших досліджень, які висвітлюють різні аспекти генезису інформаційного суспільства та інформаційної безпеки в її загальному значенні слід відзначити значну кількість наукових доробок вітчизняних науковців, серед яких О. Баранов, В. Бегма, К. Бєляков, В. Бакуменко, В. Гавловський, І. Гаврилов, В. Герасименко, О. Гладківський, М. Гуцалюк, В. Домарєв, М. Жулинський. У праці [1] проведено аналіз сучасного забезпечення захисту державних інформаційних ресурсів (ДІР) в ІТС. Проведено аналіз та систематизовано підходи до класифікації загроз інформаційним ресурсам у цілому. В монографії проведено нормативно-правовий аналіз напрямів, пов’язаних із впровадженням реєстру державних, електронних інформаційних ресурсів, досліджено шляхи подальшої реалізації проблематики, в тому числі шляхом подальшого розроблення інструментального засобу аналізу ризиків ІБ ДІР. У праці [2] розглянуто підходи і програмні рішення оцінки і контролю інформаційних ризиків як фундаментального організаційного етапу при побудові системи захисту інформації комп’ютеризованих систем. У праці [3] проведено аналіз процесу управління ризиками інформаційної безпеки в контексті забезпечення неперервності функціонування системи захисту інформації. Надана оцінка процесу управління ризиками, проаналізовані сучасні методики управління ризиками інформаційної безпеки. Запропоновано удосконалений алгоритм адаптованої методики управління ризиками при забезпеченні живучості та неперервності функціонування системи захисту інформації в інформаційно-телекомунікаційній системі. У праці [4] запропоновано та проаналізовано удосконалену методику оцінювання інформаційного ризику в автоматизованій системі. Висвітлено необхідні нормативно-правові документи інформаційної безпеки. Розглянуто роботу прототипу експертної системи, яка дозволяє оцінити рівень інформаційного ризику для певної автоматизованої системи та визначити необхідність застосування додаткових заходів інформаційної безпеки. У праці [5] проведено аналіз процесу роботи найбільш поширених моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах. Розкрито основні підходи до оцінювання ризиків інформаційної безпеки.

Таким чином проведений аналіз основних публікацій показав, що єдиного підходу щодо підвищення інформаційної безпеки інформаційно-телекомунікаційної системи Повітряних Сил не існує. Актуальним є створення біометричної системи ідентифікації доступу з застосуванням стеганографічного методу захисту інформації. З врахуванням переваги біометричних технологій (біометрії або біометрики) щодо можливості швидкої і простої ідентифікації або верифікації без спричинення незручностей індивідууму. Використання досягнень комп’ютерно-інформаційних і телекомунікаційних технологій дозволяють здійснювати ідентифікацію користувача в режимі реального часу. Біометричні технології засновані на інтеграції досягнень у галузі електроніки, інформатики, математики, медицини й біометрії, а останнім часом і на основі нанотехнологій, що дозволяє істотно зменшити габарити використовуваної апаратури для біометричних систем, що розробляються.

Мета статті полягає в аналізі методів інформаційної безпеки ІТС на основі біотехнологій.

Виклад основного матеріалу

З розвитком інформаційних технологій на сьогодні виникає проблема забезпечення інформаційної безпеки та технічного захисту інформаційних ресурсів в комп’ютеризованих системах [2]. Захищення інформації, забезпечення інформаційної безпеки повинно носити системний характер, тобто різні засоби захисту (апаратні, програмні, фізичні, організаційні). Існує велика кількість інструментів забезпечення інформаційної безпеки: засоби ідентифікації та автентифікації користувачів; засоби шифрування інформації; міжмережні екрани; віртуальні приватні мережі; засоби контентної фільтрації; інструменти перевірки цілісності вмісту дисків; засоби антивірусного захисту; системи виявлення вразливостей мереж і аналізатори мережних атак [11–12]. Особливе місце займають криптографічні методи для захисту інформації. Найпоширенішими вважаються методи кодування та шифрування інформації. Поряд з ними використовуються методи розділення та стиснення даних. У процесі захисту передачі усної інформації використовують методи аналогового скемблірування та дискретизації мови з подальшим шифруванням. Таким чином, 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 на об’єктах управління.

На основі вищесказаного пропонується метод підвищення інформаційної безпеки інформаційно-телекомунікаційної системи в якості комплексного

забезпечення інформаційної безпеки автоматизованих систем з використанням криптографічних, програмно-апаратних, технічних, правових, організаційних методів і засобів забезпечення захисту інформації [13–15]. Пропонується використовувати ідентифікаційну систему розпізнавання особи за райдужною оболонкою та реакцією очного яблука людини на подразники з використанням стеганографічного перетворення, яке складається з трифакторної аутентифікації. Метод підвищення інформаційної безпеки інформаційно-телекомунікаційної системи, в основі якого запропоновано використовувати процедуру розпізнавання особи за райдужною оболонкою та реакцією очного яблука людини на подразники, складається з наступних етапів.

Етап 1. Зчитування та фотографування обличчя кандидата для формування стеганографічного простору.

Особа, яка хоче отримати доступ до даних повинна наблизити обличчя до сканера, зафіксувати його положення і направити погляд на спеціальну мітку на дисплеї сканера. Далі камера робить знімки з швидкістю десятки кадрів у секунду, отримані зображення обробляються спеціальною програмою. Проходить етап зчитування та фотографування обличчя кандидата для формування стеганографічного простору. Фото обличчя кандидата на доступ буде використовуватись в якості контейнера, який не містить прихованої інформації. Формується множина сфотографованих даних користувача, які будуть використовуватись в якості контейнеру для стеганографічного розміщення даних.

Етап 2. Формування шаблону на основі зробленого знімку. На першому етапі обробки видаляються зображення, на якому обличчя не видно взагалі або присутні сторонні предмети, що заважають ідентифікації. За отриманими знімками відновлюється 3-D модель особи, на якій виділяються і віддаляються непотрібні перешкоди (зачіска, борода, вуса й окуляри). Потім проводиться аналіз моделі – виділяються антропометричні особливості. Проходить виділення “кола” зіниці із загального зображення очного яблука та виділення сліпих зон. Вимірюється час реакції очного яблука людини на подразники.

Етап 3. Формування контурної інформації для біометричних ознак кандидата на доступ до інформаційної системи, тобто формування множини контурів біометричних даних користувача.

$$\Omega(K) = \{K_1, ..., K_m\}. \quad (1)$$

Контури являють собою лінії, які проходять на межах однорідних областей, що задається наступною умовою:

$$| z_{\max} - z_{\min} | \le 1, \quad (2)$$

де $z_{\max}$ – елемент області зображення, який володіє найбільшим значенням;

$z_{\min}$ – елемент області зображення, який володіє найменшим значенням;

1 – поріг виявлення однорідних областей.

$$z_{\max} = \max_{1 \le i \le x} \{ z_{i,j} \}, \quad j = \overline{1, y}; \quad (3)$$

$$z_{\min} = \min_{1 \le i \le x} \{ z_{i,j} \}, \quad j = \overline{1, y}. \quad (4)$$

Найбільш поширеним способом пошуку контурів є обробка зображення ковзною маскою. Маска являє собою квадратну матрицю з коефіцієнтами. Процес обробки зображення на основі матриці називається фільтрацією або маскуванням і задається наступним функціоналом

$$M = f(Z, K), \quad (5)$$

де M – зображення, отримане в результаті обробки зображення Z на основі маски K.

Процес фільтрації заснований на поступовому просторовому переміщенні маски фільтра від елемента до елемента зображення. Значення елемента $m_{i,j}$ (відгуку фільтрації) обчислюється з використанням значень попередніх і наступних елементів у двомірній площині.

В цьому випадку значення елемента $m_{i,j}$ маски зображення M, отриманого в результаті маскування визначається за формулою

$$m_{i,j} = \sum_{\xi=i-1}^{i+1} \sum_{\tau=i-1}^{\tau+1} z_{\xi,\tau} \cdot k. \quad (6)$$

Етап 4. Введення людиною ключа (паролю). Ключ – це правило для стеганографічного перетворення зробленого системою знімку. Ключ – певна послідовність літер/цифр, відомих системі, особі, яка подає запит на ідентифікацію та адміністратору системи. За допомогою нього система розміщує дані по контейнеру, таким чином зловмисник не знатиме в які блоки контейнера занесені стеганографічні зміни. Користувач повинен ввести 2 ключі: ключова послідовність № 1 потрібна для криптографічного шифрування зображення ($\{N_1, ..., N_m\}$ – набір літер та/або цифр для формування ключової послідовності № 1); ключова послідовність № 2 потрібна для стеганографічного розміщення біометричної інформацій в контейнері ($\{M_1, ..., M_m\}$ – набір літер та/або цифр для формування ключової послідовності № 2). Отже підвищується складність доступу в систему неавторизованих користувачів.

Етап 5. Вбудовування даних в найменш значимі біти просторового представлення зображення, які обираються за допомогою введеного ключа користувачем. Вбудовування повідомлення відбувається в

молодший біт зображення, який несе в собі найменше інформації. Розмір вбудованого повідомлення може складати 1/8 загального обсягу контейнера. Наприклад, в зображення розміром 512x512 можна вбудувати 32 кБайт інформації. Якщо модифікувати два найменших біта, то пропускну спроможність можна збільшити вдвічі.

Метод вбудовування даних в спектральну область є дещо складнішим, в порівнянні з побудовою повідомлення в просторово-часову область зображення. Вбудовування інформації відбувається після дискретно-косинусного перетворення зображення.

Етап 6. Надсилання біометричного ідентифікатора кандидата на сервер розподілу та обчислень завдань у стеганографічному просторі.

Етап 7. Порівняння шаблону з наданим ідентифікатором, який проходить на технологічному етапі встановлення ідентичності на основі біометричної інформації та вирішальних правил в стеганографічному просторі.

Етап 8. Прийняття рішення системою (“свій” / “чужий”).

Таким чином, запропоновано метод підвищення інформаційної безпеки інформаційно-телекомунікаційної системи, в основі якого запропоновано використовувати процедуру розпізнавання особи за райдужною оболонкою та реакцією очного яблука людини на подразники при застосуванні стеганографічного перетворення (використання 2 ключів вводу користувачем для закриття та стеганографічного розміщення інформації).

Висновки

Досягти ефективності результату бойових дій можливо тільки шляхом створення ефективної системи управління, яка повинна функціонувати в єдиному інфокомунікаційному просторі в реальному масштабі часі, забезпечувати обробку інформації, виробку управляючих дій. При цьому проблема інформаційної безпеки системи управління набуває особливого значення в сучасних умовах широкого застосування автоматизованих інформаційних систем. Захищення інформації, забезпечення інформаційної безпеки повинно носити системний характер, тобто різні засоби захисту (апаратні, програмні, фізичні, організаційні). Існує велика кількість інструментів забезпечення інформаційної безпеки, однак єдиного підходу щодо підвищення інформаційної безпеки інформаційно-телекомунікаційної системи Повітряних Сил не існує. Пропонується створення біометричної системи ідентифікації доступу з застосуванням стеганографічного методу захисту інформації. Метод підвищення інформаційної безпеки інформаційно-телекомунікаційної системи, в основі якого запропоновано використовувати процедуру розпізнавання особи за райдужною оболонкою та реакцією очного яблука людини на подразники, складається з 7 етапів. Запропонований підхід щодо захисту інформації з використанням біометричних методів ідентифікації користувачів зменшить вплив “людського” фактору, що підвищить ефективність процедур ідентифікації та автентифікації.

Список літератури

1. Журавлев Ю.А. Правовые основы обеспечения информационной безопасности юридических лиц: автореф. дисс. на соискание ученой степени канд. юрид. наук: спец. 12.00.14. “Административное право, финансовое право, информационное право” / Ю.А. Журавлев. – М., 2009. – 26 с.

2. Закон України “Про національну програму інформатизації № 5463 від 16.10.2012 р.” [Електронний ресурс]. – Режим доступу: https://ips.ligazakon.net/document/view/z980074.

3. Брайсон Джон М. Стратегічне планування для державних та неприбуткових організацій / Джон М. Брайсон. – Л.: Літопис, 2004. – 352 с.

4. Цимбалюк В.С. Окремі питання щодо визначення категорії “інформаційна безпека” у нормативно-правовому аспекті / В.С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2004. – № 8. – С. 30-33.

5. Фурашев В.М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки / В.М. Фурашев // Інформація і право. – 2012. – № 1(4). – С. 46-56.

6. Гнідець Т.Я. Біометрія: сильна та слабкі сторони: монографія / Т.Я. Гнідець, Н.Л. Гула. – Л.: Львівський державний університет внутрішніх справ, 2014. – 326 с.

7. Мороз А.О. Біометричні технології ідентифікації людини / А.О. Мороз, К.Д. Чернов // Математичні машини і системи. – 2011. – № 1. – С. 39-45.

8. Захаров В.П. Біометричні технології в XXI столітті та їх використання органами / В.П. Захаров, В.І. Рудешко. – Л.: ЛьвДУВС, 2015. – 492 с.

9. Synthesis of combined crypto-compressed systems for providing safety video information in info-communications / V. Barannik, S. Sidchenko, I. Tupitsya, S. Stasev // 2015 IEEE East-West Design & Test Symposium (EWDTS). – Batumi, 26-29 September 2015. – P. 1-4. https://doi.org/10.1109/EWDTS.2015.7493145.

10. The method of crypto-semantic presentation of images based on the floating scheme in the basis of the upper boundaries / V. Barannik, I. Tupitsya, S. Sidchenko, R. Tarnopolov // 2nd International Scientific-Practical Conference Problems of Infocommunications Science and Technology. – Kharkiv, 13-15 October 2015. – P. 248-250. https://doi.org/10.1109/Infocommst.2015.7357326.

11. The application for internal restructuring the data in the entropy coding process to enhance the information resource security / V. Barannik, I. Tupitsya, S. Shulgin, S. Sidchenko, V. Larin // 2016 IEEE East-West Design & Test Symposium (EWDTS). – Yerevan, 14-17 October 2016. – P. 561-565. https://doi.org/10.1109/EWDTS.2016.7807749.

12. Королюк Н.О. Обґрунтування підходу щодо оцінки пропускної спроможності в інформаційно-телекомунікаційній мережі Повітряних Сил / Н.О. Королюк, Д.Ю. Голубничий, Я.Г. Поліщук // Системи озброєння і військова техніка. – 2020. – № 1(61). – С. 23-30. https://doi.org/10.30748/soivt.2020.61.03.

13. Королюк Н.О. Структурно-функціональні особливості інтелектуальних інформаційних систем військового призначення / Н.О. Королюк, О.Ю. Пермяков, С.І. Фараон // Матеріали наукового-практичного семінару "Досвід застосування військових частин та підрозділів зв'язку в ООС на сході країни з урахуванням кібернетичних впливів на інформаційно-телекомунікаційні системи". – Київ, 23 червня 2020 р. – С. 29-32.

14. Метод підвищення ефективності функціонування людино-машинної системи за рахунок підвищення якості програмного забезпечення систем підтримки прийняття рішень / О.В. Турінський, М.А. Павленко, Г.В. Пєвцов, С.В. Осієвський // Наука і техніка Повітряних Сил Збройних Сил України. – 2020. – № 4(41). – С. 125-132. https://doi.org/10.30748/nitps.2020.41.15.

15. Королюк Н.О. Удосконалення програмного забезпечення комплексів засобів автоматизації при розпізнаванні типу повітряного об'єкта / Н.О. Королюк, В.В. Синявський, Д.О. Хаустов // Системи озброєння і військова техніка. – 2017. – № 1(49). – С. 122-125.

Надійшла до редколегії 26.10.2020
Схвалена до друку 15.12.2020

Відомості про авторів:

Ряполов Іван Євгенович
кандидат технічних наук
старший науковий співробітник
Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-3139-1644

Кметюк Яна Ігорівна
курсант Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0003-4097-8997

Дубинець Марина Сергіївна
курсант Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-1160-5721

Information about the authors:

Ivan Ryapolov
Candidate of Technical Sciences
Senior Research Associate
of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-3139-1644

Yana Kmetiuk
Cadet of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0003-4097-8997

Maryna Dubynets
Cadet of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-1160-5721

МЕТОД ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ БИОТЕХНОЛОГИЙ

И.Е. Ряполов, Я.И. Кметюк, М.С. Дубинец

В результате проведенного анализа установлено, что проблема информационной безопасности системы управления приобретает особое значение в современных условиях широкого применения автоматизированных информационных систем. Обеспечение информационной безопасности должно носить системный характер. В результате проведенного исследования установлено, что существует большое количество инструментов обеспечения информационной безопасности, имеют недостатки, связанные с защитой и дискриминацией, возможностью подделки пароля, невыполнением инструкций по созданию безопасного пароля пользователем, существованием и наличием в свободном доступе специализированных приложений для подбора и взлома паролей. Человеческий фактор является основным недостатком данных систем. Единого подхода по повышению информационной безопасности информационно-телекомуникационных систем Воздушных Сил не существует. Предлагается создание биометрической системы идентификации доступа применением стеганографического метода защиты информации. Метод повышения информационной безопасности информационно-телекоммуникационной системы, в основе которого предложено использование процедуры распознавания личности по радужной оболочке и реакции глазного яблока человека на раздражители. Предложенный подход по защите информации с использованием биометрических методов идентификации пользователей уменьшит влияние "человеческого" фактора, повысит эффективность процедуры идентификации и аутентификации.

Ключевые слова: *биотехнологии, идентификация, аутентификация, верификация, системы доступа, шаблон, сопоставления, хранилище данных.*

METHOD FOR IMPROVING INFORMATION SECURITY INFORMATION AND TELECOMMUNICATION SYSTEM BASED ON BIOTECHNOLOGIES

I. Ryapolov, Ya. Kmetyuk, M. Dubynets

As a result of the analysis it is established that the problem of information security of the control system acquires special significance in modern conditions of wide application of automated information systems. Ensuring information security should be systemic. The study found that there are a large number of information security tools that have shortcomings related to protection and discrimination, the possibility of password forgery, failure to follow instructions for creating a secure password by the user, the existence and availability of specialized applications for selection and hacking passwords. The human factor is the main disadvantage of these systems. There is no single approach to improving the information security of the information and telecommunication system of the Air Force. It is proposed to create a biometric access identification system using the steganographic method of information protection. A method of improving the information security of the information and telecommunications system, which is based on the use of iris recognition and human eyeball response to stimuli. The proposed approach to information protection using biometric methods of user identification will reduce the impact of "human" factor identification and authentication procedures. It is proposed to use the identification system of facial recognition by the iris and the reaction of the human eyeball to stimuli using steganographic transformation, which consists of three-factor authentication. The method of increasing the information security of the information and telecommunication system, based on which it is proposed to use the procedure of face recognition by the iris and the reaction of the human eyeball to stimuli, consists of the following stages. The proposed approach to information protection using biometric methods of user identification will reduce the impact of the "human" factor, which will increase the efficiency of identification and authentication procedures.

***Keywords**: biotechnology, identification, authentication, verification, access systems, template, mapping, data warehouse.*