

РЕФЕРАТ

Магістерська дисертація: 94 с., 24 рис., 20 табл., 10 додатків, 57 джерел.

Актуальність. В даний час більшість комп'ютерних систем і онлайн веб-сайтів ідентифікують користувачів виключно за допомогою таких облікових даних, як паролі і пін-коди (персональні ідентифікаційні номери). Ці системи піддають своїх користувачів крадіжкам особистих даних - злочину, в якому хакери видають себе за законних користувачів, щоб зробити шахрайську діяльність. Хакери використовують інші посвідчення шляхом крадіжки облікових даних або за допомогою комп'ютерів, що увійшли в систему, які залишаються без нагляду.

Основною загрозою для організацій є крадіжки особистих даних, які вчинені внутрішніми користувачами, які належать до організації. Зазвичай хакер отримує доступ до конфіденційної інформації, яка може використовуватися для промислового шпигунства, вимагання тощо. Недоліки методів ідентифікації, які покладаються лише на облікові дані, призводять до введення методів перевірки користувачів, які використовуються разом із ідентифікацією користувачів на основі посвідчень. Методи верифікації підтверджують ідентичність користувачів відповідно до поведінкової та фізіологічної біометрії.

Верифікація може виконуватися один раз під час входу в систему або безперервно протягом всього сеансу. В останньому випадку біометричні вимірювання користувача приймаються з регулярними інтервалами, коли користувач входить в систему і порівнюється з еталонними даними, які були зібрані заздалегідь. Звичайні поведінкові методи біометрії включають характеристики взаємодії між користувачем та пристроями вводу, такими як миша та клавіатура.

Основним недоліком методів перевірки користувачів, які базуються на фізіологічній біометрії, є те, що вони вимагають спеціальних пристроїв, таких як датчик відбитків пальців та сканер сітківки ока, які є дорогими та не завжди доступними. Хоча перевірка відбитків пальців стає все більш поширеною в ноутбуках, вона все ще не досить популярна і не може бути інтегрована до використання у веб-застосунках. Крім того, відбитки пальців можна скопіювати.

Актуальність даної теми обумовлена розробкою нових моделей і методів розпізнавання користувача у КС, що не вимагають спеціальних призначених пристроїв, оскільки вони використовують таке обладнання як стандартний маніпулятор (миша, сенсорний маніпулятор, сенсорний екран).

Робота присвячена побудові нової інформаційної технології (ІТ), що забезпечує високоякісне розпізнавання користувача комп'ютерної системи (КС) за траєкторіями руху курсору «миші» з використанням апарату прихованої марківської моделі (ПММ).

Мета дослідження – розроблення прикладного програмного забезпечення, підсистеми ідентифікації користувачів, що базується на покращенні ефективності захисту конфіденційних даних від несанкціонованих дій шляхом за допомогою використання рухів курсору та апарату прихованих моделей Маркова.

Мета дисертаційної роботи визначає необхідність розв'язання таких **завдань**:

- аналіз існуючих методів біометричного розпізнавання;
- аналіз моделей і методів ідентифікації та аутентифікації користувачів у комп'ютерних системах;
- модифікувати методи прихованих моделей Маркова, для найкращого їх використання в системі, що розробляється;
- проектування програмного забезпечення;
- реалізація розроблених алгоритмів у вигляді програмного забезпечення для ідентифікації та аутентифікації користувачів за допомогою динаміки курсора та апарату ПММ.

Об'єкт дослідження – моделі і методи ідентифікації користувачів у комп'ютерних системах.

Предмет дослідження – метод ідентифікації користувача через траєкторії руху курсора «миші» із подальшою аутентифікацією.

Методи дослідження. Для досягнення поставлених завдань використано методи аналізу, синтезу, математичного моделювання, чисельних методів, моделювання інформаційних систем, об'єктно-орієнтованого аналізу і програмування.

Наукова новизна одержаних результатів полягає у вдосконаленні методу автентифікації користувачів шляхом використання біометричних даних за траєкторією руху курсора, який, на відміну від існуючих підходів, розширює функціональні можливості засобів автентифікації, що уможлиблює підвищення ефективності системи захисту.

Практичне значення одержаних результатів. Отримані результати можуть бути використані при створенні прикладних програмних систем електронної комерції, інтернет-банкінгу, корпоративних застосувань, що містять конфіденційну інформацію, або навіть звичайні домашні комп'ютери, що містять певну персональну інформацію і мають вихід до глобальних мереж.

Особистий внесок здобувача. Усі наукові результати, подані у дисертації, одержані здобувачем особисто.

Апробація результатів дисертації. Основні результати дисертаційної роботи апробовані на таких конференціях: VII Всеукраїнській науково-практичній конференції «Наукова Україна: проблеми сучасності та перспективи майбутнього»; науково-технічній конференції «The actual problems of informatization of management decisions» (APIMD 2018) – м. Київ.: НТУУ «КПІ ім. Ігоря Сікорського»

Публікації. Основні результати дисертаційного дослідження опубліковано у 2 наукових працях, із них: 1 – одноосібна; 2 публікації – матеріали конференцій [1, 2].

БИОМЕТРИЧНЕ РОЗПІЗНАВАННЯ, СТАТИСТИЧНІ МОДЕЛІ, ПРИХОВАНІ МАРКІВСЬКІ МОДЕЛІ