УДК 004.052.42

д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
д.т.н., доц. **Бойченко О. В.** (ОДАТРЯ)

ОЦІНКА ВІРОГІДНОСТІ ДАНИХ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ

У статті запропоновано застосування методу оцінки вірогідності даних інформаційної системи спеціального призначення на основі пошарового модульного контролю захищеності програмного забезпечення автоматизованої системи управління.

Основою методу є застосування покрокових криптографічних перетворень шарів спеціального програмного забезпечення інформаційної системи, що дозволяє проводити оперативне оцінювання потоків даних, що циркулюють в системі.

Розробленням методу створені умови для забезпечення оперативної оцінки вірогідності даних інформаційної системи спеціального призначення, що дозволяє підвищувати показник рівня контролю за інформаційними ресурсами до 27%.

Ключові слова: автоматизована система управління, інформаційні ресурси, вірогідність даних, пошаровий модульний контроль, криптографічні перетворення.

Постановка проблеми. З певною часткою впевненості можна стверджувати, що невдачі й розчарування, пов’язані з впровадженням ряду нових автоматизованих інформаційних систем, обумовлені, насамперед, відсутністю єдиного підходу до питань

збору, систематизації й аналізу даних.

Аналіз останніх досліджень і публікацій. Практика сучасного досвіду експлуатації інтегрованих інформаційно-пошукових систем спеціального призначення, переконливо показує, що успіх в інформаційному забезпеченні діяльності організацій та установ, може бути досягнута тільки за умови охвату всього комплексу проблем, пов'язаних зі здобуванням, обробкою й аналізом інформації. Зазначене підтверджується дослідженнями таких вчених як Тихонов В. А., Татарченко И. В., Соловьев Д.С., Барсуков В. С. та ін. [1-3].

Постановка завдання. При цьому важливо відзначити, що накопичення й зберігання даних – це не визначальна ланка в загальному технологічному ланцюжку. Більш того, ті дані й відомості, що накопичуються, взагалі не є інформацією в її функціональному значенні, і в силу цього цінність їх досить умовна. Однак відомості, що накопичуються в автоматизованих системах, і дані є, безумовно, найпершим інформаційним ресурсом, і, таким чином, завдання полягає в тому, щоб зробити цей «внутрішній» інформаційний ресурс досить ємним, змістовним і максимально достовірним.

Виклад основного матеріалу. Сучасні досягнення науки й технології сьогодні знаходять саме активне застосування у світовій практиці автоматизованого управління та контролю діяльності установ та організацій. Особливу роль у процесах контролю та захисту даних автоматизованих систем управління відведено спеціалізованим системам ідентифікації людини.

Біометрія – це методи автоматичної ідентифікації, засновані на фізіологічних або поведінкових характеристиках. Прикладами фізіологічних характеристик є відбитки пальців, форма руки, характеристика особи, райдужна оболонка ока, тощо. Розпізнавання за допомогою біометричних технологій припускає порівняння раніше внесеного біометричного зразка з біометричними даними, що знову надійшли.

Робота усіх біометричних систем заснована, як правило, на типовому алгоритмі, що узагальнено можна представити в наступному вигляді:

- запис – фізичний або поведінковий зразок запам'ятовується системою;
- виділення шаблону – унікальна інформація виноситься зі зразка й складається біометричний шаблон;
- порівняння – збережений зразок порівнюється із представленим;
- збіг / розбіжність – система вирішує, чи збігаються біометричні зразки, і виносить рішення.

Біометрія пропонує швидкий, зручний, точний, надійний і порівняно ощадливий спосіб ідентифікації з величезною кількістю найрізноманітніших застосувань. Немає такої єдиної біометричної технології, що підійшла б для усіх потреб.

Усі біометричні системи мають свої переваги й недоліки. Насамперед, будь-яка система повинна бути заснована на характеристиці, що є помітною й унікальною. Є достатня кількість наукових даних, що підтверджують вкрай низьку ймовірність наявності абсолютно ідентичних відбитків пальців, характеристик побудови обличчя або райдужної оболонки ока. Інший аспект – наскільки «дружелюбна» конкретна технологія. Технологічний процес повинен бути швидким, простим, що заподіює мінімальної незручності людині.

Принцип роботи системи розпізнавання заснований на спеціальному алгоритмі перекладу зображень у цифровий формат, при цьому здійснюється пошук обличчя в кадрі й визначення характерних ознак його побудови – так званих «реперних точок» (розташування й форма очей, вилиці, ширина перенісся, губ та інші). У результаті кожна особа описується унікальним набором параметрів, причому з деяким надлишком. Для ідентифікації з високим ступенем точності досить не більше 40 характеристик, тоді як система звичайно задає кілька тисяч оцінних параметрів. Фотографія й цифровий опис обличчя заносяться до бази даних, якою надалі здійснюється пошук.

Ефективність біометричних систем ідентифікації людини, що використовують методи автоматизованої обробки зображення обличчя, багато в чому визначається дотриманням ряду обов'язкових вимог, що забезпечують кількісні і якісні характеристики базової фото-

теки.

Основними джерелами біометричних шаблонів бази даних інформаційних систем спеціального призначення (ІСПР) є:

- фотопортрет особи, представлений у цифровому виді (графічний файл);
- фотографія портретного типу (для подальшого сканування);
- цифровий «відеопотік» (окремий фрагмент у вигляді медіафайлу, або відеосигнал, що надходить у реальному часі).

Тому що процес ідентифікації являє собою встановлення тотожності невідомого об'єкта відомому на підставі збігу ознак, будь-якому фотозображенню, що буде брати участь у процесі біометричного впізнання, повинні бути встановлені унікальні атрибути. У зв'язку з цим фотозображення перед виділенням унікальної інформації для складання біометричного шаблону (процес кодування), поміщається до інтегрованого банку даних з обов'язковою прив'язкою до відповідного об'єкта обліку.

Як показав проведений аналіз, більшість систем, що використовують біометричні технології, побудовані за принципом самодостатності, тобто функціонально обмежені виконанням завдань ідентифікації або верифікації об'єкта, без можливості одержання більш повної інформації про об'єкт аналізу, що значною мірою знижує ефективність використання подібних систем. Крім того, використання самодостатніх, вузькоспеціалізованих систем біометричної ідентифікації ускладнює їхню інтеграцію в існуючий єдиний інформаційний простір.

Головною відмінною рисою сучасних ІСПР є повна інтеграція в єдине інформаційне поле інформаційного банку даних (ІБД), а функціональна класифікація процесів розпізнавання образів виглядає такий чином [4]:

• ідентифікація (процес встановлення тотожності об'єкта або особистості за сукупністю загальних і приватних ознак, здійснювана з метою вирішення питання про те, чи є даний об'єкт шуканим):

- ідентифікація з використанням фотографічних зображень;
- ідентифікація (упізнання) за методом словесного портрета;
- ідентифікація у відеопотоці;
- мобільна ідентифікація;

• верифікація (процес порівняння нового біометричного зразка з раніше збереже ним, при якому біометрична система намагається підтвердити або спростувати, що ця людина дійсно та, за кого себе видає):

- верифікація (порівняння двох об'єктів);
- множинна верифікація (автоматизований процес порівняння об'єкта верифікації з декількома зразками для одержання ступеня схожості між ними).

Розширення функціональних можливостей єдиної інтегрованої інформаційної системи спеціального призначення забезпечується за допомогою габітоскопії – криміналістичної технології на основі програмного модулю, що функціонує у складі комплексної системи ідентифікації особистості ІСПР.

Підсистема ідентифікації особистості за методом словесного портрету використовується для введення й коректування установчих реквізитів на осіб, а також для проведення ідентифікації осіб шляхом порівняння їх біометричних параметрів з раніше введеними в базу даних.

Підсистема дозволяє врахувати практично всі можливі випадки наявності або відсутності додаткової якісної інформації про те, як виглядає особа, яка ідентифікується. Опис зовнішності будується на базі близько 50 параметрів, що використовуються для спрощення процедури розпізнавання. Для прискорення роботи також впроваджено різні схеми оптимізації обчислень і обробки даних.

Набір реквізитів для введення й пошуку в підсистемі ідентифікації особистості за словесним описом заснований на розпізнавальній карті й містить у собі основні біометричні дані людини, опис його зовнішності, характерних прикмет, стану зубів і одягу. Характерні

прикмети докладно описуються з вказівкою їх виду й областей тіла, на яких вони розташовані.

Заставою позитивного результату створення й подальшого розвитку розглянутої системи, є відмова її розроблювачів від помилкової стратегії реформування системи інформаційного забезпечення на основі вирішення завдання автоматизації процесів. При цьому інформаційні технології автоматизують (багаторазово прискорюють) існуючий процес з усіма його недоліками, але завдання проектування кардинального підвищення фективності не ставиться. Крім того, популярний реінжиніринг програмного забезпечення, коли на основі сучасних технологій відбувається переписування застарілих інформаційних систем без зміни самих процесів, що автоматизуються.

Отримані наукові результати. Актуальним питанням є шлях системного вирішення проблеми процесу «пожвавлення» інформаційних масивів і перетворення їх у реальне джерело інформаційного аналізу в діяльності організацій та установ не «власними силами», ніж простим впровадженням готових закордонних рішень.

Зазначене вказує на можливість створення додаткових проблем, пов'язаним із загрозами ресурсам інформаційної системи через суттєве зниження достовірності та вірогідності даних.

Вирішення зазначеної проблеми можливо із застосуванням методу покрокового криптографічного перетворення шарів спеціального програмного забезпечення інформаційної системи на основі технології пошарового проектування [5].

Метод передбачає проведення тестових випробувань щодо порівняння реакції інформаційної системи на несанкціоновані впливи до та після впровадження технології пошарового проектування (рис. 1).

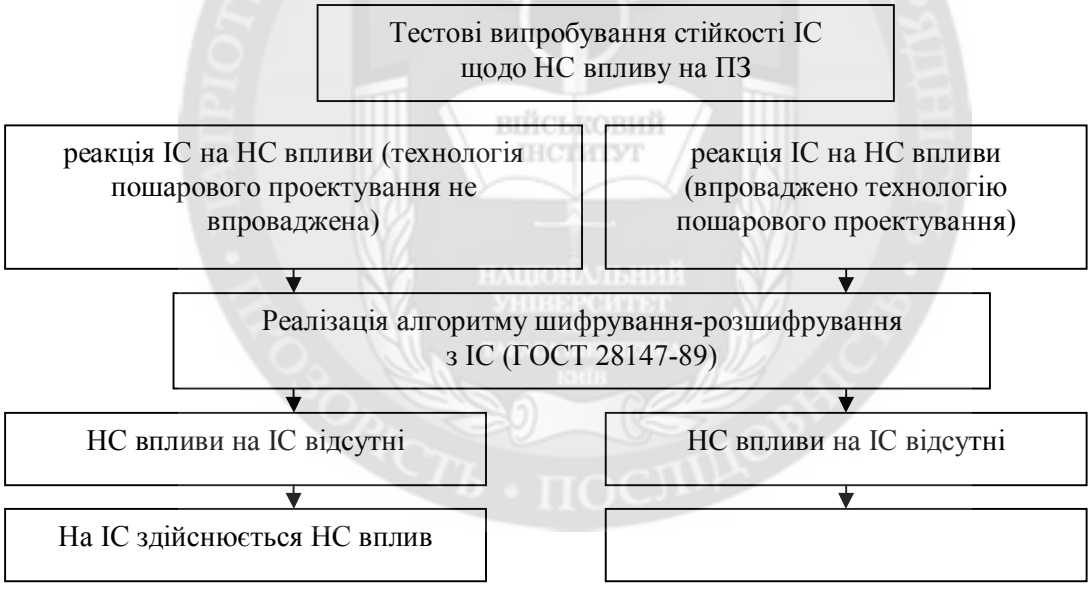

Рис. 1. Алгоритм тестових випробувань стійкості ПЗ ІС до несанкціонованих впливів

За кожним напрямом алгоритму тестових випробувань стійкості ПЗ ІС до несанкціонованих впливів здійснюється послідовно три етапи операцій (рис. 2, рис. 3).

Проведення несанкціонованих дій з модифікації програмних блоків при шифруванні (конкретно в прикладі: у 10-м пункті криптографічних перетворень замість циклічного зрушення вліво на 11 розрядів із-за несанкціонованої модифікації виробляється циклічне зрушення на 12 розрядів), несанкціонована модифікація відстежується при самоконтролі і маркер $S_7 = 0$, що також відбивається і в маркері $S_8 = 0$, який не пов'язаний безпосередньо з модифікованим програмним блоком.

Завдяки непрямому зв'язку в обчислювальній структурі потоку, покрокова циклова структура захисту за розробленою технологією приводить до встановлення несанкціонованої дії (маркер $S = 0$) та контролю рівня вірогідності даних інформаційної системи.

Рис. 2. Етапи тестових випробувань стійкості ПЗ ІС до несанкціонованих впливів

Рис. 3. Результати тестових випробувань стійкості ПЗ ІС до несанкціонованих впливів

Результати досліджень визначають перспективність запропоновано застосування методу оцінки вірогідності даних інформаційної системи спеціального призначення на основі пошарового модульного контролю захищеності програмного забезпечення автоматизованої системи управління.

Висновки. Застосування покрокових криптографічних перетворень шарів спеціального програмного забезпечення інформаційної системи дозволяє проводити оперативну оцінку потоків даних, що циркулюють в системі. Розробленням методу створені умови для забезпечення оперативної оцінки вірогідності даних інформаційної системи спеціального призначення, що дозволяє підвищувати показник рівня контролю за інформаційними ресурсами до 27%.

Отримані наукові результати можуть знайти подальше застосування під час наукових досліджень в напрямку розроблення методичних основ оцінки вірогідності даних інформаційних систем спеціального призначення.

ЛІТЕРАТУРА:

1. Тихонов В.А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты / В.А. Тихонов, В.В. Райх. – М.: Гелиос АРВ, 2006. – 245 с.

2. Татарченко И.В. Концепция интеграции унифицированных систем безопасности / И.В. Татарченко, Д.С. Соловьев // Системы безопасности. – М., 2009. - № 1 (73). – С. 86-89.

3. Барсуков В. С. Интегральная защита информации / В.С. Барсуков // Системы безопасности. – М., 2012. – №5. – С.45-49.

4. Татарченко Н.В. Биометрическая идентификация в интегрированных системах безопасности / Н.В. Татарченко, С.В. Тимошенко // Специальная техника. – М., 2002. – С.44-48.

5. Бойченко О.В. Моделі і методи підвищення стійкості інформаційної системи спеціального призначення: Дис. д-ра техн. наук: 05.13.06. – К., 2013. – 298 с.

Без рецензії.

д.т.н., проф. Ленков С.В., д.т.н., доц. Бойченко О.В.

ОЦЕНКА ДОСТОВЕРНОСТИ ДАННЫХ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ

В статье предложено применение метода оценки достоверности данных информационной системы специального назначения на основе послойного модульного контроля защищенности программного обеспечения.

Основой метода является применение пошаговых криптографических превращений слоев специального программного обеспечения информационной системы, что позволяет проводить оперативную оценку потоков данных, которые циркулируют в системе.

Разработкой метода созданы условия для обеспечения оперативной оценки достоверности данных информационной системы специального назначения, что позволяет повышать показатель уровня контроля информационных ресурсов до 27%.

Ключевые слова: автоматизированная система управления, информационные ресурсы, достоверность данных, послойный модульный контроль, криптографические превращения.

S. Lenkov. O. Boitchenko

ESTIMATION AUTHENTICITY OF INFORMATION AUTOMATED CONTROL SYSTEM OF MANAGEMENT

In the article application method of estimation authenticity of information the informative system the special setting is offered on the basis of layer module control protected of software.

Basis of method is application of incremental cryptographic transformations of layers the special informative system software, which allows conducting the operative estimation flows of data which circulate in the system.

Development of method is create terms for providing of operative estimation authenticity of information of the informative system the special setting, that allows to promote the index level of control of informative resources to 27%.

Keywords: automated control system of management, informative resources, authenticity of information, layer module control, cryptographic transformations.