Індустрію 4.0 може стати джерелом нових можливостей для своїх організацій. Індустрія 4.0 змінює зміст і співвідношення категорій споживання, очікувань, цінності, якості і споживчого досвіду, що вимагає трансформації традиційних поглядів і підходів до менеджменту якості [7].

У статті кратко представлені етапи на шляху перетворення підприємств на підприємства потреби четвертої промислової революції.

Завдяки збору й аналізу даних в реальному часі та штучного інтелекту, та здатності всіх компонентів виробничої лінії «спілкуватися» один з одним, виробництво може бути дійсно ефективним і персоналізованим, відповідно до потреб клієнтів.

Завдяки посиленню автоматизації для людей з'явиться час для зосередження уваги на більш складних завданнях. Людський дотик буде важливим для забезпечення ефективного вирішення проблем і підтримки управління в цифровому середовищі.

ЛІТЕРАТУРА

1. Ortiz J.H. Industry 4.0 Current Status and Future Trends Edited. London, United Kingdom. 2020. P. 19 – 81.
2. Soldatos J. Introduction to Industry 4.0 and the Digital Shopfloor Vision. // Marousi, GR15125, Greece. 2019. – P. 2 –18.
3. Sergi B., Popkova E., Bogoviz A., Litvinova T. Understanding industry 4.0: AI, the Internet of things, and the future of work. // Emerald Publishing. 2019. P. 47 –133.
4. Пуха Ю. «Индустрия 4.0»: создание цифрового предприятия. // Всемирный обзор реализации концепции «Индустрия 4.0» за 2016 год. 2016. С. 2 –10.
5. Кокорев Д.С., Юрин А.А. Цифровые двойники: понятие, типы и преимущества для бизнеса // Colloquium-journal. Голопристанський міськрайонний центр зайнятості, 2019. №. 10 (34). С. 1–5.
6. Yudina M. Industry 4.0: Opportunities and Challenges. // Fourth Industrial Revolution. 2017. P. 3 –23.
7. Салимова Т. А., Ватолкина Н. Ш. Менеджмент качества в условиях перехода к индустрии 4.0 //Стандарты и качество. 2018. Т. 972. №. 6. С. 58.

Науковий керівник: *Сотник Світлана Вікторівна, к.т.н., доцент кафедри КІТАМ, Харківського національного університету радіоелектроніки*

УДК 004.3; 004.9

РОЗРОБКА СТРУКТУРИ АВТОМАТИЗОВАНОЇ СИСТЕМИ БЛОКУВАННЯ ДОСТУПУ ДО ВІЗУАЛЬНОЇ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ HID-ПРИСТРОЮ

Божко П. М.

Харківський національний університет радіоелектроніки

Україна, 61166, Харків, пр. Науки, 14

E-mail: pavlo.bozhko@nure.ua

Анотація: У роботі виконано аналіз проблеми захисту конфіденційної інформації. Розглянуто способи та методи крадіжки інформації, проведено аналіз наявних конструкцій і характеристик автоматичних систем контролю доступу до інформації. Запропоновано структурну схему системи. На її основі вибрано апаратні модулі та датчики. В результаті була розроблена схема електрична принципова автоматизованої системи.

Ключові слова: автоматизована система, інформація, контроль, доступ, блокування.

DEVELOPMENT OF AN AUTOMATED SYSTEM STRUCTURE FOR BLOCKING ACCESS TO VISUAL INFORMATION USING A HID-DEVICE

P. Bozhko
Kharkiv National University of Radioelectronics
Ukraine, 61166, Kharkiv, Nauky av.,14
E-mail: pavlo.bozhko@nure.ua

Annotation: The analysis of the problem of confidential information protection is performed in the work. Methods and techniques of information theft are considered, the analysis of existing designs and characteristics of automatic systems of access control to information is carried out. The structural scheme of the system is offered. Based on it, hardware modules and sensors are selected. As a result, a circuit diagram of the basic principle of the automated system was developed.

Key words: automated system, information, control, access, blocking.

АКТУАЛЬНІСТЬ РОБОТИ. На сьогодні однією із найважливіших проблем у житті будь-якого користувача комп`ютера є захист своїх збережених даних від шахраїв та зловмисників.

Ще кілька десятків років тому проблема захисту цифрової інформації користувача комп'ютера не стояла так гостро, адже її використання було досить малим. Але з кожним роком цифрова інформація все більше і більше проникає у життя людей. Сьогодні навіть рецепт у лікаря можна отримати у вигляді цифрового документа. Одночасно з ростом використання цифрової інформації виникає потреба в її захисті, особливо актуальною ця проблема стала після низки хакерських атак на комп'ютерні ресурси світових компаній. Зараз майже у кожної людини є персональний комп'ютер (ПК), кожна людина має велику кількість конфіденційної інформації, яку необхідно захищати від зловмисників та сторонніх «поглядів». Через це розробка автоматизованої системи блокування доступу до візуальної інформації з використанням HID-пристрою стане одним із варіантів для зручного захисту від сторонніх «поглядів» на інформацію на екрані комп'ютера.

Використання в розроблюваній системі захисту інформації HID-пристрою має ряд переваг: проста конструкція та невеликі розміри, компактність, що дозволяє його залишити непомітним та розмістити в будь-якому зручному для користувача місці. Завдяки магніту його можна розмістити в підвішеному стані, наприклад під столами або біля інших предметів інтер`єру. Область застосування для пристрою універсальна: це може бути як домашнє використання, так і користування у робочому процесі. Область використання може бути різноманітною, адже він в будь-якому місці зможе виконувати свою основну функцію, де є користувач і комп`ютер.

ВСТУП. Інформація – це усвідомлені відомості про навколишній світ, які є об'єктом зберігання, перетворення, передачі і використання. Існують три основні методи отримання інформації з комп'ютера:

– безконтактний;

– контактний, за допомогою технічних засобів встановлених в контрольованих ланцюгах;

– за допомогою впроваджених програмних модулів в програмному забезпеченні (ПЗ), через мережі.

Так як пристрій, що розроблюється буде захищати від витоку різних видів інформації, яка буде міститися на ПК, то було розглянуто основні канали витоку та способи знімання інформації, а також способи захисту. Основними каналами витоку конфіденційної інформації є [1]:

– вібраційні канали;

– електроакустичні канали;

– оптико-електронні канали;

– параметричні канали;

– візуально-оптичні канали;

– електромагнітні канали.

У вібраційних каналах (структурних каналах) витоку інформації середовищем поширення акустичних сигналів є конструкція будівель (стіни, стелі, підлоги), труби водо- і теплопостачання, каналізації та інші тверді тіла. Основним способом знімання інформації в цьому випадку є вібродатчики.

Методи знімання інформації: через використання структурного звуку в стінах або перекриттях; витік через мережі опалення, газо- і водопостачання.

Засобами захисту інформації при використанні вібраційних каналів є захисні фільтри.

Електроакустичні канали витоку інформації зазвичай утворюються шляхом перетворення акустичних сигналів в електричні за двома основними напрямками: шляхом "високочастотного нав'язування" і шляхом перехоплення через допоміжні технічні засоби і системи. Найчастіше подібний канал витоку інформації використовують для перехоплення розмов, що ведуться в приміщенні, через стаціонарний (дротовий) телефон, який має вихід за межі контрольованої зони.

Методи знімання інформації:

– знімання інформації шляхом наведень і "нав'язування";

– знімання інформації через використання "телефонного вуха";

– витік через канал охоронно-пожежної сигналізації.

Одним із основних способів знімання інформації є підключення до допоміжних технічних засобів і систем (телефон, датчики пожежної сигналізації, гучномовці ретрансляційної мережі).

Методи і засоби захисту інформації:

– використання спеціальних пристроїв, що приховують канал зв’язку;

– відключення телефонних апаратів від лінії при проведенні в приміщенні конфіденційних розмов;

– установка в телефонній лінії спеціального пристрою захисту, який автоматично відключає телефон від лінії при встановленій телефонній трубці;

– використання методу виводу з ладу закладних пристроїв або їх модулів, що зчитують сигнал, шляхом подачі в лінію високовольтних імпульсів.

При опроміненні лазерним променем вібруючих в акустичному полі тонких дзеркальних поверхонь, таких як скло вікон, дзеркал, картин тощо, створюється оптико-електронний (лазерний) канал витоку акустичної інформації. Відбите лазерне випромінювання модулюється по амплітуді і фазі і приймається приймачем оптичного випромінювання, при демодуляції якого виділяється мовна інформація. Для перехоплення мовної інформації з даного каналу використовуються радіолокаційні системи, що працюють, як правило, в ближньому інфрачервоному діапазоні і відомі як "лазерні мікрофони" [1]. Дальність перехоплення складає кілька сотень метрів.

Метод знімання інформації – лазерне зчитування акустичної інформації з вікон.

Спосіб знімання інформації – за допомогою використання "лазерних мікрофонів".

Методи і засоби захисту інформації: звукоізоляція вікон; встановлення на скло вікон генераторів завадних вібрацій або віброізоляція.

Канали витоку графічної інформації реалізуються технічними засобами і надають інформацію у вигляді зображень об'єктів або копій документів, одержуваних шляхом спостереження за об'єктом, зйомки об'єкта і копіювання документів. Залежно від умов спостереження, зазвичай, використовуються відповідні технічні засоби, в тому числі: оптика, телекамери. Для документування результатів спостереження проводиться зйомка об'єктів. Для зняття копій документів використовуються електронні і спеціальні (закамуфльовані) фотоапарати. Для дистанційного знімання видової інформації використовують сховані відеокамери, або здійснюють відео-зйомку з будівель розташованих поблизу.

Методи знімання інформації: спостереження; фотографування; відеозйомка об'єкта.

Способи знімання інформації: знімання інформації з використанням прихованих відеокамер; використання закамуфльованої техніки (фотоапарата, відеокамери); спостереження за об'єктом з сусідніх будівель.

Методи і засоби захисту інформації: пошук схованих пристроїв запису (відеокамери, фотоапарати); екранування приміщення; використання жалюзі або штор.

Для електромагнітних каналів витоку характерними є побічні електромагнітні випромінювання елементів технічних засобів обробки інформації. Носієм інформації є електричний струм, сила, напруга, частота або фаза якого змінюються згідно із законом інформаційного сигналу. Електромагнітні випромінювання на частотах роботи генераторів технічних засобів обробки інформації допоможуть захиститися від витоку інформації.

ПОСТАНОВКА ЗАДАЧІ. Інформаційну систему в загальному випадку можна уявити як інформаційний простір та пристрій, що оброблює інформацію. Обчислення розбиваються на окремі модулі, розташовані в інформаційному просторі. Схему виконання обчислень можна представити таким чином: пристрій, що оброблює дані, під керівництвом виконавчої програми може звертатися до інформаційного простору, зчитуючи і редагуючи його [2].

Серед засобів захисту інформації важливе місце займають апаратно-програмні інструменти контролю доступу до комп'ютерів – електронні замки, пристрої введення ідентифікаційних ознак (ПВІО) і відповідне ПЗ. Спільне застосування ПВІО і електронного замка дає можливість спорудити перед зловмисником дві лінії захисту, які наведено на рис. 1 [3].

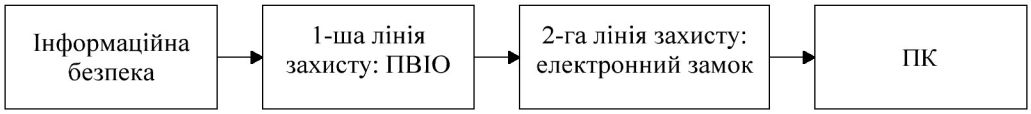

Рисунок 1 – Дві лінії захисту [3]

Доступ до інформаційних ресурсів комп'ютера користувач отримує після успішного виконання процедур ідентифікації і автентифікації. Ідентифікація полягає в розпізнаванні користувача за властивими або наданими йому ідентифікаційними ознаками. Перевірка приналежності пред'явленого ним ідентифікатора (підтвердження автентичності) проводиться в процесі автентифікації.

У апаратно-програмних засобах контролю доступу до комп'ютерів ідентифікація і автентифікація, а також ряд інших важливих захисних функцій, здійснюються за допомогою електронного замка і ПВІО до завантаження операційної системи [4]. До складу апаратних засобів ПВІО входять ідентифікатори і зчитувальні пристрої. Сучасні ПВІО класифікуються по виду ідентифікаційних ознак і за способом їх зчитування, які наведено на рис. 2.

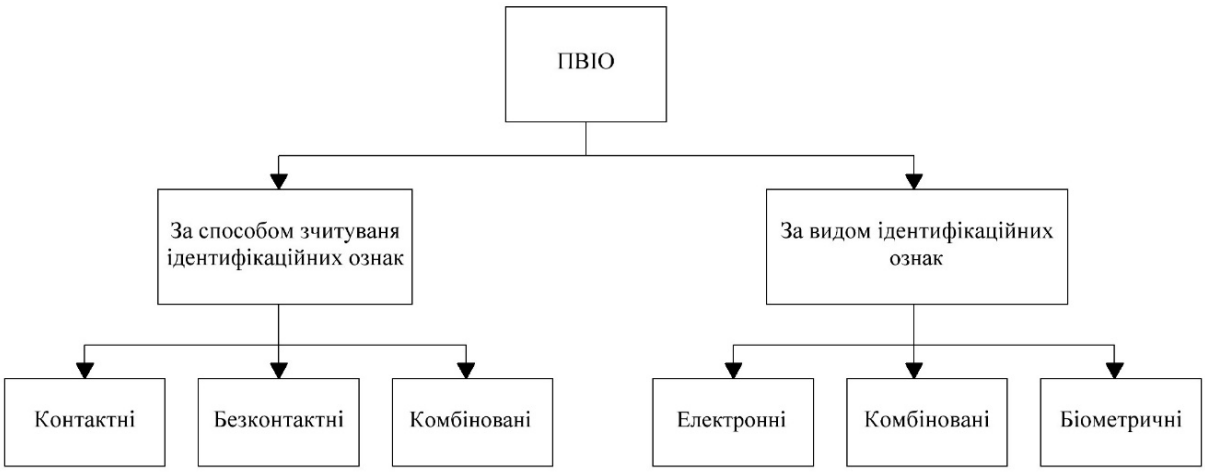

Рисунок 2 – Класифікація ПВІО [4]

За способом зчитування вони поділяються на: контактні, дистанційні (безконтактні) і комбіновані.

Контактне зчитування ідентифікаційних ознак передбачає безпосередню взаємодію ідентифікатора і зчитувача – проведення ідентифікатора через зчитувач або зчитування на відстані.

Безконтактний (дистанційний) спосіб зчитування не вимагає чіткого позиціювання ідентифікатора і зчитувача.

Комбінований спосіб має на увазі поєднання обох методів зчитування та одночасне їх використання.

В електронних ПВІО ідентифікаційні ознаки представляються у вигляді коду, записаного в мікросхему пам'яті ідентифікатора. В біометричних пристроях ідентифікаційними ознаками є індивідуальні фізичні ознаки людини (відбитки пальців, геометрія долоні, малюнок сітківки ока, голос, динаміка підпису і т. д.).

РІШЕННЯ ЗАДАЧІ. Після проведення аналізу розроблено структурну схему системи контролю доступу до роботи на ПК, в котрій наведено основні елементи, з яких буде складатися пристрій (рис. 3).

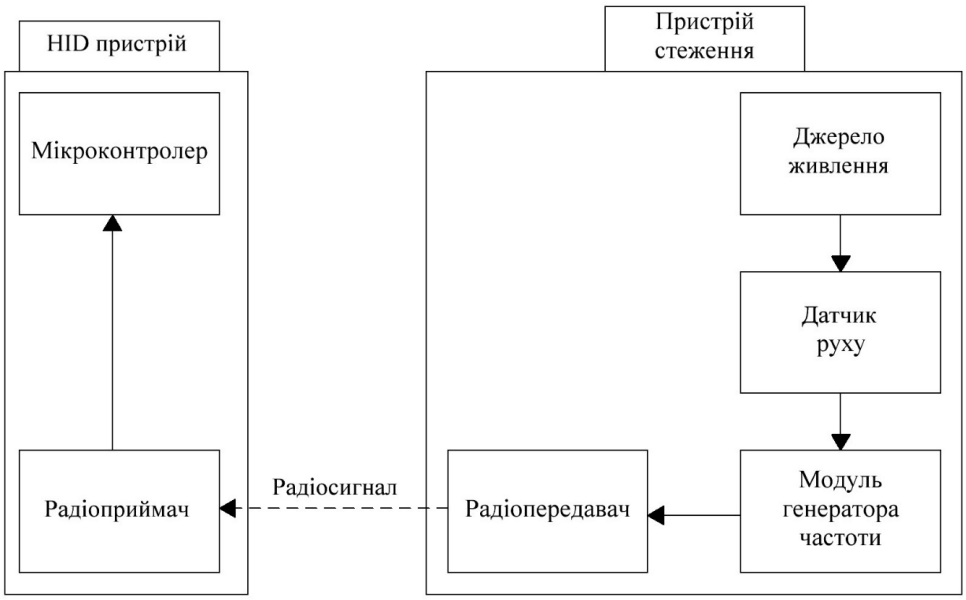

Рисунок 3 – Структурна схема комп’ютерно-інтегрованої системи контролю доступу

Для розроблення системи було обрано плату ATINY85 Digispark. Мікроконтролер пристрою використовується як виконавчий пристрій, він отримує інформацію вад радіоприймача, який працює на частоті 433 МГц та керує системами захисту на ПК [5]. Разом ці два компоненти утворюють модуль керування.

Пристрій стеження слідкує за простором та надсилає значення датчика руху до модуля керування за допомогою радіопередавача. Модуль керування після отримання сигналу починає виконувати визначену послідовність команд. Ці команди можна налаштовувати за необхідністю. У розроблюваній системі такою командою буде блокування ПК. Однак це створює деякі незручності, а саме: встановлення захисного пароля під час початку використання ПК, а також реагування датчика пристрою на будь-який рух. Для уникнення цих недоліків потрібно паралельно використовувати систему розпізнавання обличчя для того, щоб комп’ютер не переходив у режим блокування, коли датчик помітить саме власника цього ПК.

Через те, що конструкція складається з двох модулів потрібно два джерела живлення. Для модуля керування як джерело живлення буде використано мережу 5В комп'ютера, а для живлення пристрою стеження буде використано два акумулятори типорозміру 18650, які забезпечать досить великий час автономної роботи.

Для передачі інформації через радіоканал обрано радіо модуль, який складається з двох незалежних частин: приймача SYN480R та передавача SYN115. Цей радіоканал має досить хороші показники стійкості сигналу та завадостійкості.

Як пристрій слідкування за рухом використовується піроелектричний інфрачервоний (PIR) датчик руху. Ці датчики мають невеликі габарити, малу ціну, споживають мало енергії, практично не схильні до зносу і дуже часто використовуються в системах сигналізації, де і зарекомендували себе. 3D-моделі корпусу пристрою стеження будуть розроблені в САПР SolidWorks та роздруковані на 3D-принетрі. Програма керування написана на мові C++ з використанням середовища Arduino IDE для більш простого налаштування мікроконтролеру.

ВИСНОВКИ. Таким чином, у роботі проведено ретельний аналіз предметної області, зокрема видів та методів витоку цифрової інформації. Описано можливі способи захисту від витоку. Розроблено структурну схему автоматизованої системи блокування доступу до візуальної інформації й обрано та описано її основні складові частини.

У процесі подальшої роботи необхідно буде проаналізувати та визначити переваги та недоліки аналогів розроблювальної системи; розробити конструкцію макета; побудувати 3D-моделі усіх компонентів, що будуть друкуватися на 3D-принтері; розробити програмне забезпечення для керування системою контролю доступу; налагодити радіозв'язок між модулем стеження та виконавчим модулем.

ЛІТЕРАТУРА

1. Основы информационной безопасности и защиты информации [Електронний ресурс]. – Режим доступу: www/ URL: https://sites.google.com/site/anisimovkhv/learning/kripto/ lecture/tema1 – 01.11.2021 р. – Загол. з екрану.
2. Способ защиты визуальной информации на дисплее компьютера и устройство для его реализации [Електронний ресурс]. – Режим доступу: www/ URL: https://findpatent.ru/patent/ 212/2126988.html – 01.11.2021р. – Загол. з екрану.
3. Маскирование цифровой визуальной информации: термин и основные определения [Електронний ресурс]. – Режим доступу: www/ URL: https://cyberleninka.ru/article/n/maskirovanie-tsifrovoy-vizualnoy-informatsii-termin-i-osnovnye-opredeleniya/viewer. – 01.11.2021 р. – Загол. з екрану.
4. Защита цифровой информации [Електронний ресурс]. – Режим доступу: www/ URL: https://remonline.ua/ru/blog/protection-of-information-in-modern-world/ – 02.11.2021 р. – Загол. з екрану.https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsion-noj-bezopasnosti
5. Плата розробника ATtiny85 USB від Digispark [Електронний ресурс]. – Режим доступу: www/ URL: https://arduino.ua/prod1985-plata-razrabotchika-attiny85-usb-ot-digispark – 02.11.2021 р. – Загол. з екрану.
6. Міні датчик руху PIR [Електронний ресурс]. – Режим доступу: www/ URL: https://uamper.com/Мини-пироэлектрический-инфракрасный-датчик-движения-PIR – 02.11.2021 р. – Загол. з екрану.

Науковий керівник: *Бабак Ірина Миколаївна, доцент, к.т.н., доцент кафедри КІТАМ Харківського національного університету радіоелектроніки.*