МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА
СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

"На правах рукопису"
УДК 681.3.06

«До захисту допущено»
Завідувач кафедри
_____ Шуклін Г.В.
(підпис) (ініціали, прізвище)
«____» _____ 2023р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 Кібербезпека

РОЗРОБКА ГЕНЕРАТОРА РАДІОЗАВАД ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНОГО КОМП`ЮТЕРА

Студент групи СЗД – 41 Тунік Олександр Олександрович _____
(підпис)

Керівник к.т.н., доц. Котенко Андрій Миколайович _____
(підпис)

Нормоконтроль: ст. викладач Зозуля Сергій Анатолійович _____
(підпис)

Київ – 2023

«ЗАТВЕРДЖУЮ»

Завідувач кафедри

_____ Шуклін Г.В.
(підпис) (ініціали, прізвище)

«__» _____ 2023р.

ЗАВДАННЯ

на атестаційну роботу магістра

студенту Туніку Олксандру Олександровичу

1. Тема роботи: Розробка генератора радіозавад для захисту персонального комп`ютера, керівник Котенко Андрій Миколайович, к.т.н., доцент., затверджені наказом вищого навчального закладу від «24» лютого 2023 року № 26.

2. Термін здачі студентом оформленої роботи «30» травня 2023 р.

3. Предмет дослідження: методи просторової локалізації та ідентифікації об'єктів інформаційної діяльності.

4. Об`єкт дослідження: процеси витоку інформації по технічним каналам на при роботі персонального комп`ютера.

5. Мета роботи: створення системи інформаційного захисту на об'єкті інформаційної діяльності при роботі на персональному комп`ютері за допомогою генератора радіозавад.

6. Перелік питань, які мають бути розроблені:

1) аналіз типів інформації, яка витікає по технічним каналам при роботі персонального комп`ютера;
2) аналіз загроз щодо несанкціонованого доступу до конфіденційної інформації на об'єкті інформаційної діяльності при роботі персонального комп`ютера;
3) аналіз технології радіозавад при роботі персонального комп`ютера;
4) створення системи інформаційного захисту прироботі на персональному комп`ютері за допомогою генераторів радіозавад.

Презентація виконана на 10 слайдах для подання за допомогою світло проекторів та комп’ютерних засобів.

Дата видачі завдання «24» листопада 2023 р.

Керівник: Котенко Андрій Миколайович _____

Завдання прийняв до виконання: Тунік Олександр Олександрович _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	**Примітка**
1	Підбір науково-технічної літератури	02.03.23	Виконано
2	Обґрунтування актуальності теми роботи	10.03.23	Виконано
3	Написання першого розділу роботи	до 01.04.23	Виконано
4	Написання другого розділу роботи	до 01.05.23	Виконано
5	Написання третього розділу роботи	до 30.05.23	Виконано
6	Перевірка роботи на плагіат + передзахист	До 02.06.23	Виконано
9	Захист роботи	08.06.23	
10	Випуск	30.06.23	

Студент О. О. Тунік

Керівник роботи А. М. Котенко

РЕФЕРАТ

Бакалаврська кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел і має 57 сторінок основного тексту, 30 рисунків, 1 таблиця. Список використаних джерел містить 22 найменувань.

Метою роботи є створення системи інформаційного захисту на об'єкті інформаційної діяльності при роботі на персональному комп`ютері за допомогою генератора радіозавад аналіз типів інформації, яка витікає по технічним каналам при роботі персонального комп`ютера. Проведено аналіз загроз щодо несанкціонованого доступу до конфіденційної інформації на об'єкті інформаційної діяльності при роботі персонального комп`ютера. Здійснено аналіз технології радіозавад при роботі персонального комп`ютера. Створено систему інформаційного захисту при роботі на персональному комп`ютері за допомогою генераторів радіозавад.

ANNOTATION

The bachelor's thesis consists of an introduction, three chapters, conclusions, and a list of references and includes 57 pages of the main text, 30 figures, and 1 table. The list of references includes 22 items.

The purpose of the work is to create a system of information protection at the object of information activity when working on a personal computer using a radio interference generator, to analyze the types of information that flows through technical channels when a personal computer is working. An analysis of threats to unauthorized access to confidential information at the object of information activity when working on a personal computer is carried out. The analysis of radio interference technology in the operation of a personal computer is carried out. A system of information protection when working on a personal computer with the help of radio interference generators is created.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОІД – об’єкт інформаційної діяльності

ІзОД – інформація з обмеженим доступом

RFID – Radio Frequency Identification - «радіочастотна ідентифікація»

ОС – операційна система

ЕМС – електромагнітна сумісність

ПБ – політика безпеки

ПРД – правила розмежування доступу

ІБ – інформаційна безпека

ІС – інформаційна система

ІТ – інформаційні технології

ІТС – інформаційно-телекомунікаційна система

СКУД – система контролю та управління доступом

ВСТУП

Увага до питань інформаційної безпеки зростає, дослідження в цій сфері свідчать про намагання збалансувати зусилля щодо зниження ризиків з підвищенням ефективності діяльності.

У теперішній час у багатьох областях діяльності існує необхідність у системах бесконтактної двумірної локалізації об’єків у приміщеннях. Такі системи знаходять застосування при пошуку та відстеження об’єктів у приміщеннях, наприклад, товарів на складах, книг у бібліотеках, працівників на підприємствах. При цьому широко використовуємі глобальні супутникові навігаційні системи непридатні для вирішення такої задачі.

Перспективним направленням просторової локалізації об’єктів у закритих приміщеннях є застосування технології радіочастотної ідентифікації (radio frequency identification ((RFID)). У такому випадку на об’єктах локалізації встановлюють спеціальні RFID - мітки, місцезнаходження, яких може бути визначено шляхом аналізу інформації, яка отримується від міток.

В даній дипломній роботі пропонується використовувати технологію RFID для визначення місцезнаходження матеріальних носіїв ІзОД, для недопущення крадіжки їх злочинцями. Тобто запобігти витоку ІзОД матеріально-речовим каналом.

На підставі цього можна зробити висновок, що тема атестаційної роботи, присвячена запобіганню витоку ІзОД матеріально-речовим каналом за рахунок використанням технологій RFID, є актуальною.

РОЗДІЛ 1 ЗАГРОЗИ ІНФОРМАЦІЇ НА ОБЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ТА ЗАХИСТ ВІД НИХ

1.1. Правовий режим доступу до інформації

У Законі України «Про інформацію» наведено терміни:

захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [1].

Режим доступу до інформації - передбачений правовими нормами порядок одержання, використання, поширення, зберігання інформації [1].

За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом [1], а остання -на конфіденційну і таємну.

У більшості випадків інформація є відкритою, обмеження права на одержання подібної інформації забороняється. Держава здійснює контроль за режимом доступу до інформації.

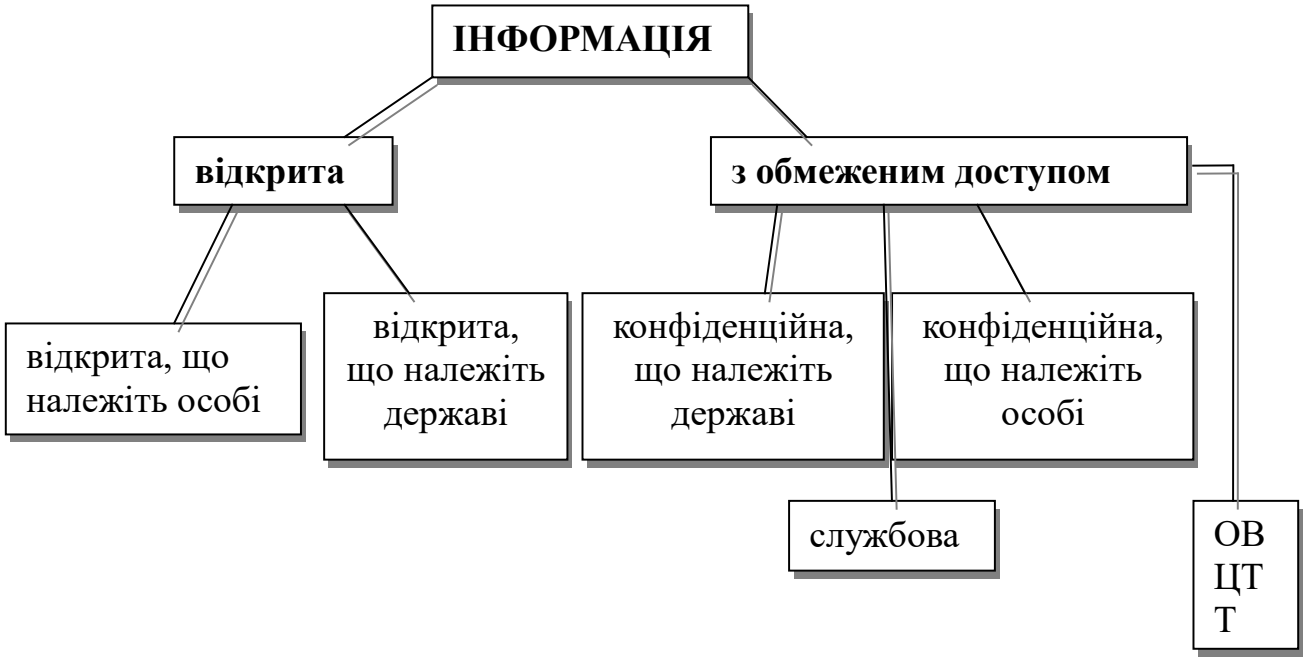

Рис.1.1. Розподіл інформації за режимом правового доступу до неї

Доступ до відкритої інформації забезпечується шляхом:

- систематичної публікації її в офіційних друкованих виданнях (бюлетенях, збірниках);
- поширення її засобами масової комунікації;
- безпосереднього її надання заінтересованим громадянам, державним органам та юридичним особам [1].

Порядок і умови надання громадянам, державним органам, юридичним особам і представникам громадськості відомостей за запитами встановлюються Законом України «Про інформацію» або договорами (угодами), якщо надання інформації здійснюється на договірній основі [1].

Обмеження права на одержання відкритої інформації забороняється законом. Переважним правом на одержання інформації користуються громадяни, яким ця інформація необхідна для виконання своїх професійних обов'язків [1].

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденціальну і таємну [1].

Конфіденціальна інформація - це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов [1].

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденціальної, та встановлюють для неї систему (способи) захисту[1].

Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої являє загрозу життю і здоров'ю людей [1].

До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі [1].

Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до закону «Про інформацію» [1].

Секретна інформація за ступенем секретності (категорія, яка харектеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою) поділяється на іформацію «особливої важливості», «цілком таємно», «таємно»).

Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно значимою, тобто якщо вона є

предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист [1].

У Законі «Про інформацію» інформаційні запити поділяються на два види:

- доступу до офіційних документів;
- надання письмової або усної інформації.

Під інформаційним запитом (надалі - запитом) щодо доступу до офіційних документів розуміється звернення з вимогою про надання можливості ознайомлення з офіційними документами. Запит може бути індивідуальним або колективним. Він подається у письмовій формі [1].

Громадянин має право звернутися до державних органів і вимагати надання будь-якого офіційного документу, незалежно від того, стосується цей документ його особисто чи ні, крім випадків обмеження доступу [1].

У запиті повинно бути зазначено прізвище, ім'я та по батькові запитувача, документ, письмова або усна інформація, що його цікавить, та адреса, за якою він бажає одержати відповідь.

Органи законодавчої, виконавчої та судової влади України, їх посадові особи зобов'язані надавати інформацію, що стосується їх діяльності, письмово, усно, по телефону чи використовуючи публічні виступи своїх посадових осіб [1]. Термін вивчення запиту на предмет можливості його задоволення не повинен перевищувати десяти календарних днів.

Відмова в задоволенні запиту доводиться до відома запитувача у письмовій формі з роз'ясненням порядку оскарження прийнятого рішення.

У відмові має бути зазначено:

1) посадову особу державної установи, яка відмовляє у задоволенні запиту;
2) дату відмови;
3) мотивовану підставу відмови.

Відмову або відстрочку задоволення запиту може бути оскаржено. У разі відмови в наданні документа для ознайомлення або відстрочки задоволення запиту запитувач має право оскаржити відмову або відстрочку до органу вищого рівня. Якщо на скаргу, подану до органу вищого рівня, дається негативна відповідь, запитувач має право оскаржити цю відмову до суду. У

разі, коли запитувач звернувся до суду, обов'язок доводити законність відмови чи відстрочки задоволення запиту покладається на відповідача - державну установу [1].

Не підлягають обов'язковому наданню для ознайомлення за інформаційними запитами офіційні документи, які містять у собі:

- інформацію, визнану у встановленому порядку державною таємницею;
- конфіденціальну інформацію;
- інформацію про оперативну і слідчу роботу органів прокуратури, МВС, СБУ, роботу органів дізнання та суду у тих випадках, коли її розголошення може зашкодити оперативним заходам, розслідуванню чи дізнанню, порушити право людини на справедливий та об'єктивний судовий розгляд її справи, створити загрозу життю або здоров'ю будь-якої особи;
- інформацію, що стосується особистого життя громадян;
- документи, що становлять внутрівідомчу службову кореспонденцію (доповідні записки, переписка між підрозділами та інше), якщо вони пов'язані з розробкою напряму діяльності установи, процесом прийняття рішень і передують їх прийняттю;
- інформацію, що не підлягає розголошенню згідно з іншими законодавчими або нормативними актами. Установа, до якої звернуто запит, може не надавати для ознайомлення документ, якщо він містить інформацію, яка не підлягає розголошенню на підставі нормативного акта іншої державної установи, а та державна установа, яка розглядає запит, не має права вирішувати питання щодо її розсекречення;
- інформацію фінансових установ, підготовлену для контрольно-фінансових відомств [1].

1.2. Дослідження загроз інформації на об’єктах інформаційної діяльності

Захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі [3].

Несанкціоновані дії щодо інформації в системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства [3].

Технічний захист інформації (ТЗІ) - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації [3].

Мета ТЗІ - запобігання витоку або порушенню цілісності та доступності інформації, що підлягає захисту.

Для забезпечення технічного захисту інформації в Україні створена система технічного захисту інформації.

Забезпечення захисту інформації в системі покладається на власника системи. Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним [3].

Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган. Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом [3].

Захисту від витоку технічними каналами на ОІД (об'єкт інформаційної діяльності) підлягає інформація, що становить державну таємницю. Захист іншої ІзОД від витоку технічними каналами на ОІД здійснюється за рішенням розпорядника цієї інформації. Створення комплексу ТЗІ передбачає проведення організаційних, інженерних і технічних заходів на ОІД, а саме:

- озвучення ІзОД (при проведенні нарад, під час показів зі звуковим супроводженням кіно- і відеофільмів тощо);
- здійснення обробки ІзОД технічними засобами (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання ІзОД тощо);

- обіг іншої ІзОД при проектуванні, будівництві, експлуатації об'єктів, виробництві технічних засобів тощо.

Для захисту інформації створюються системи (комплекси) захисту інформації. За для забезпечення роботи з матеріальними носіями секретної та службової інформації і їх зберігання (в робочий та неробочий час) створюються системи охорони (здіснюється організація режиму доступу). Системи захисту інформації будуються за такими етапами:

I – визначення і аналіз загроз для інформації;

II – розробка політики безпеки та плану захисту інформації;

III – розробка технічного завдання на створення системи захисту інформації (ЗІ);

IV – розробка проекту системи ЗІ;

V – упровадження системи ЗІ;

VI – оцінювання захищеності інформації;

VII – введення системи ЗІ в експлуатацію.

Рис. 1.2 Структура витоку інформації

Відповідно до інформаційної діяльності на ОІД можна виділити такі первинні джерела небезпечного сигналу:

- акустично людиною в процесі розмови або засобами відтворення чи підсилення звуку;
- технічні засоби та системи, що обробляють інформацію;

- монітори засобів електронно – обичислювальної техніки, екрани. Секретні документи з надрукованим текстом тощо, на яких візуалізується інформація;
- за допомогою фішингу та аналогічних методів кібератак.

За носієм інформації та принципом формування небезпечного сигналу відокремлюються такі технічні канали витоку інформації:

- електромагнітні канали витоку інформації, до яких відносяться канали побічних електромагнітних випромінювань.
- електричні канали витоку інформації, до яких відносяться канали побічних електромагнітних наведень на комунікації, канали зняття інформації з лінії провідного зв’язку та тому подібні;
- параметричні канали витоку інформації, до яких відносяться, канали «паразитної» модуляції та тому подібні.

Причини виникнення електричних каналів витоку інформації [6]:

— гальванічні зв'язки з'єднувальних ліній ТЗПІ (технічний засіб перетворення інформації) з лініями ДТЗС (допоміжні технічні засоби системи) і сторонніми провідниками;
— наведення побічних електричних випромінювань ТЗПІ на з'єднувальні лінії ДТЗС і сторонні провідники;
— наведення побічних електричних випромінювань ТЗПІ на ланцюзі електроживлення і заземлення ТЗПІ;
— «просочування» інформаційних сигналів у колі електроживлення і заземлення ТЗПІ.

Однією з основних причин каналу витоку інформації лінями заземлення є типи заземлення, які рідко вдається виконати відокремлено. Поєднуючи разом функції однієї системи провідників і провідних поверхонь все це призводить до того, що по ним відбуваються різні струми, які і можуть бути небезпечні. Небезпечними потоками є і зворотні струми для різних сигналів основних технічних засобів і систем (ОТЗС), а також струми, які обумовленні наведеними небезпечними сигналами на лінію заземлення.

Витік інформації по ланцюгах заземлення може виникнути [6]:

- при наявності рознесених точок заземлення інформативних ланцюгів в разі утворення в різних точках системи заземлення

різниці потенціалів і виникнення в результаті цього струмів в ланцюгах заземлення;

- при великому значенні опору заземлення;
- внаслідок недосконалості екранів, що приводить до асиметрії ліній відносно екрана і виникнення в ланцюзі між корпусом екрана та землею інформативних струмів.

Одними з найнебезпечніших для витоку мовної інформації є акустооптоелектронні (лазерно-акустичні) канали. Функціонування об’єктів інформаційної діяльності пов’язане з циркуляцією в них акустичної мовної інформації. Розповсюдження акустичних хвиль від джерела небезпечного сигналу за межі контрольованої зони і можить спричинити витік інформації.

Дані канали утворилися шляхом перехопленя мовних сигналів з ОІД акустичними мікрофонами направленої дії чи акустичними антенами засобів технічної розвідки, що встановлюються в зоні видомості вікон. Акустичні хвилі можуть проходити через конструкцію з ьаких причин, як:

1. Якщо стіна чи інша конструкція є не достатньо масивна, то під дією акуустичного тиску вона починає коливатися та створює тиск за межами ОІД.
2. Щілини (замкові отвори в дверях, зазори між дверима), мікрощілини, вентиляції. Великі пройми будуть сприяти безперешкодному розповсюдженню акустичного сигналу.

Акустоелектричні канали будуть виникати, якщо буде відбуватися паразитне перетворення акустичних сигналів в електричні за принципом мікрофонного ефекту.

Лазерний акустичний канал утворюється шляхом дистанційного поза межами КЗ зняття лазерними засобами акустичної розвідки вібраційних коливань, що спричиняються акустичним полем, тобто небезпечним мовним сигналом. Як відбувається даний витік інформації, за допомогою деяких предметів, що мають оптичні властивості віддзеркалення і приводять до вібрації. Якщо на них(зовні) спрямувати лазерний промінчик, то він віддзеркалиться від поверхні у вигляді промінчика, модульованого тремтінням від сигналу вібрації і розповсюджується далі.

Відео-Акустичний мікрофон. Це метод який дозволяє відтворити звукову інформацію з відео за допомогою запису інформації на високо-якісну швидкісну камеру зі сповільненою зйомкою. За достатньої якості і швидкості відео можливе відтворення звуку завдяки спостереженням за вібраціями обєктів які легко піддаються їх впливу наприклад рослини. Цей метод можливий для використання назаміну лазерно-акустичному оскільки лазер простіше виявити через сильне направлене випромінення [22].

Найбільш відомим та одним з досих простих, а також оснащеним найсучаснішими технічними засобами розвідки є візуально-оптичне спостереження. Даний вид містить:

- Достовірною і точно видобутою інформацією;
- Швидким отриманням інформації;
- Доступною реалізацією;
- Документальне отримання відомостей (фото, відео).

Оптичні методи є одні з найстаріших методів, які допомагають отримати інформацію. Саме до них, можемо віднести:

- візуальні методи спостереження;
- фотозйомка;
- відеозйомка.

На практиці розвідку широко можуть використовувати для отримання інформації з відходів виробничої та трудової діяльності [6]. Особливостю матеріально-речового каналу, що і дає перевагу над іншими каналами, являє саме специфіка джерела і носіїв. В даному випадку суб’єктами являються люди і матеріальні об’єкти (макро- і мікрочастини), які мають чіткі просторові межі локалізації.

Джерелами інформації, що є основними в матеріально-речовому каналі витоку інформації є [6], [7], [8]:

- чернетки різних документів і макети матеріалів, вузлів, блоків, пристроїв, що розробляються в ході науково-дослідних і дослідно-конструкторських робіт, які ведуться в організації;
- вийшли з ладу магнітні та інші носії інформації ПЕОМ, на яких під час експлуатації містилася інформація з обмеженим доступом;
- секретні бібліотеки;

- інші місця зберігання матеріальних носіів ІзОД.

Однією з важливих загроз є добування інформації з магнітних носіїв, яка вважається стертою. При «стиранні» файла не відбувається знищення інформації на носії. Знищується лише заголовок та шлях до нього на носії. Через деякий час на місця попередніх записів може бути записана нова інформація, яка переорієнтує намагніченість доменів. Поверх даних, на яких не було здійснено запис, залишаються і можуть бути доступними і відновленими за допомогою штатних засобів на програмному рівні. Щоб знищити інформацію, існують засоби які дозволяють перезаписати знищувану інформацію довільними значеннями на магнітному полотні.

Інформація може бути перенесена такими суб'єктами та середовищами, як:

- співробітник;
- повітряні атмосферні маси;
- рідке середовища.

Витік інформації через матеріально-речові канали витоку інформації може бути здійснене через:

- розкрадання носіїв інформації;
- внутрішні канали витоку (через обслуговуючий персонал);
- виробничі та технологічні відходи (папір з принтерів, виробничі відходи підприємств);
- погано прихована видова інформація про хід виробничого процесу на підприємстві.

1.3. Використання технологій радіочастотної ідентифікації у системах захисту інформації від витоку матеріально-речовим каналом

Щоб запобігти витік інформації за допомогою матеріально-технічних каналів на практиці використовується фізична та технічна складова служби безпеки організації [6], [8] (рис. 1.4).

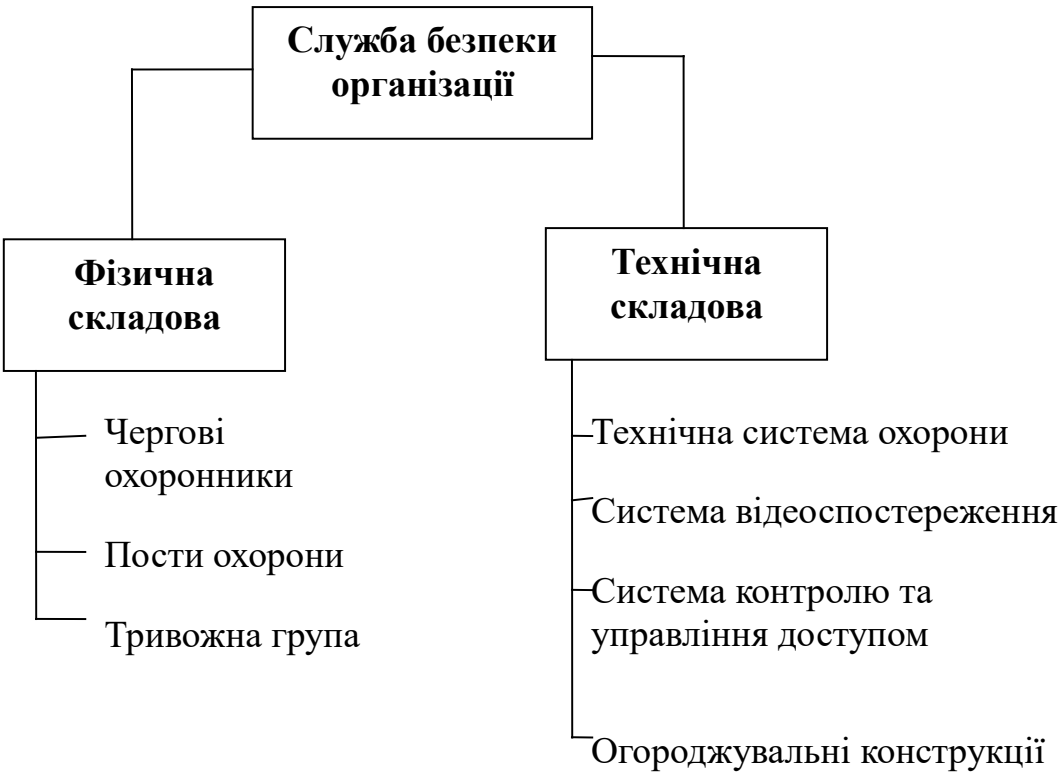

Рис.1.4. Складові, що запобігають витоку інформації матеріально-речовим каналом

За допомогою системи відеоспостереження, яка є програмно-апаратним комплексом та призначена для запису відеоінформації, а також передає її до місця перегляду та зберігання інформації [8].

На об’єктах охорони, встановлюється технічна система охорони, яка обов’язково задовольняє і є в комплексі з силами фізичної охорони і системою інженерних споруджень [6], [8].

Елементами технічного захисту об’єктів являється:

- Засоби виявлення;
- Засоби управління доступом до об’єктів;
- Засоби збору, обробки;
- Технічні засоби відеоспостереження;
- Засоби для виконання розвідки;

Для визначення повноважень доступу людей і автотранспорту на територіях, потрібно використовувати системи контролю доступу (СКД). Дана

інформація, яка збирається записується в базу даних та в подальшому може аналізуватися.

За допомогою функції контролю за переміщенням, яка і використовується для унеможливлення несанкціонованого переміщення матеріальних носіїв ІзОД. Якщо буде виявлено дане переміщення, тобто витік сатеріально-речовими каналами, локалізувати місцезнаходження матеріального носія ІзОД. Отже, для вирішення даної задачі пропонується використовувати технологію радіочастотної ідентифікації (RFID).

Висновки до першого розділу

У першому розділі було досліджено та встановлено інформацію за режимом правового доступу. Виявлено якою буває інформація і як саме забезпечується шлях до різних типів інформаціє та як він контролюється.

Також, досліджено можливі загрози для інформації, які можуть виникати на об’єктах інформаційної діяльності. Визначено яких правил потрібно дотримуватися, щоб запобігти витоку інформації матеріально-технічним каналом.

В межах даної роботи було складено та вказано приклад методу для виявлення та вирішення несанкціонованого переміщення матеріальних носіїв ІзОД.

РОЗДІЛ 2 ТЕХНОЛОГІЇ РАДІОЧАСТОТНОЇ ІДЕНТИФІКАЦІЇ

2.1. Сутність технології радіочастотної ідентифікації

RFID-мітка (Radio Frequency Identification) -це мініатюрний запам’ятовуючий пристрій. В основі пристрою використовується мікрочип, який і зберігає інформацію, та антена, яка відповідає за передачу та отримання даних. В більшості випадків дані прилади не потребують живлення. Пам’ять RFID-мітки зберігає унікальну інформацію, що містить дані та номер. Коли відбувається попадання в реєстраційну зону, інформація сприймається зчитувачем та здійснюється її зчитування.

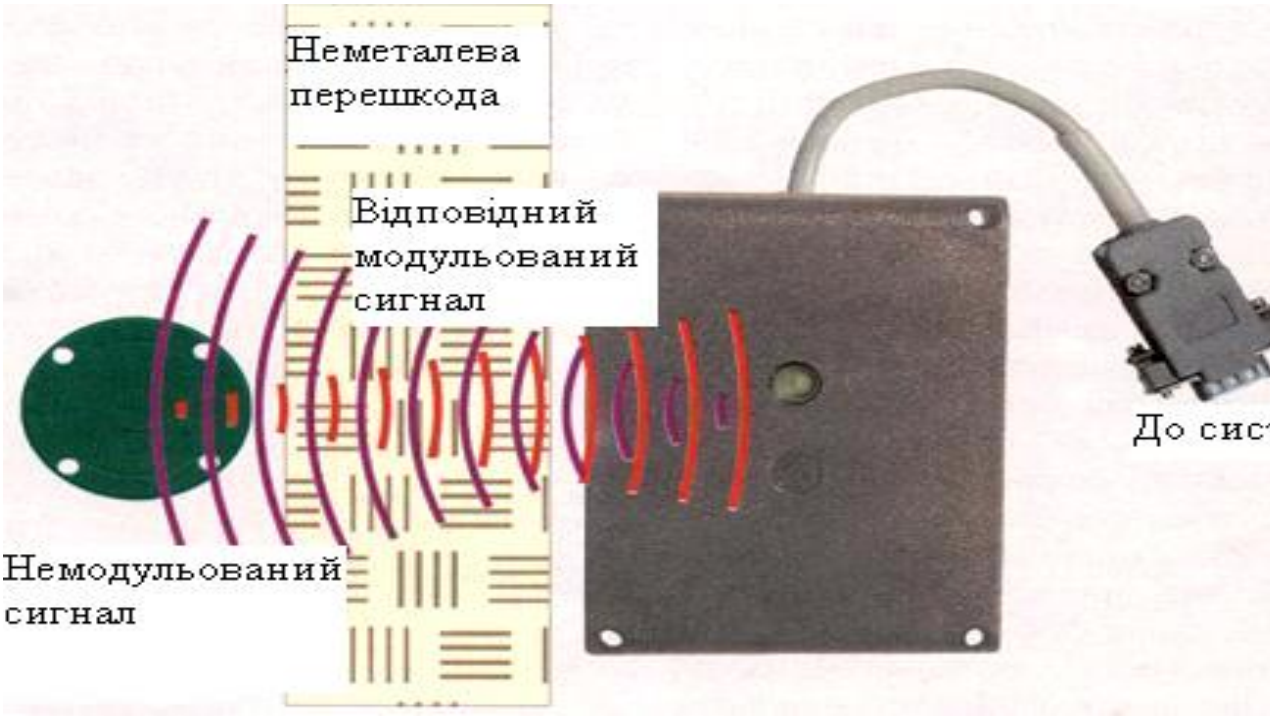

Рис. 2.1. Принцип дії радіочастотної ідентифікації

Дана технологія активно застосовується при контролюванні переміщення різних об'єктів, в інтелектуальних автоматизованих рішеннях. RFID-мітка працюють без помилок, швидко та надійно. Дана технологія використовується в різних галузях, таких як:

1. Галузь виробництва. RFID-мітка гарантує якісний рівень продукції.

2. Склади. Прискорює приймання та відвантаження товарів, а також може підвищувати рівень прозорості та надійності операцій.
3. Бібліотеки. В книжкових сховищах спрощується система видачі книг споживачам, що допомагає уникнення крадіжок.

RFID-система складається з:

- Мітки, пристрій, який зберігає та передає дані.

- Зчитувач. Сполучаючи з системою, вони працюють в незалежному режимі.

- Система обліку. Це програми, що накопичують і аналізують інформацію.

Де і коли використовують технологію RFID?

Сфера застосування карт досить широка:

- студентські картки;

- ключі від готелів;

- абонементи в фітнес-клуби;

- громадський транспорт;

Спочатку повернемося до перших транспондерів, які були пластиковими інтелектуальними ідентифікаційними картами – ІК (SmartCard) з контактами згідно ISO-7816 «Ідентифікаційні картки». Системи, які використовують ІК почали називатися ІК-системами, а технології обслуговування об'єктів ІК-технологіями. Специфічні елементи ІК-систем є лише ІК і зчитувачі, а все інше являється типовим відповідником автоматизованих систем. Отже, можемо зробити висновок, що ІК-технології можуть досить просто упроваджено практично в будь-яку технологію.

ІК-технології забезпечують можливість автоматично обслуговувати індивідуально кожен об'єкт на всіх етапах його життєвого циклу. Тому, щоб це все виконувалося потрібно лише побудувати відповідну автоматизовану систему з інфраструктурою зчитувачів.

ІК-технологія спирається на ієрархічну побудову інформаційних даних при обслуговуванні об'єктів (рис. 2.2) [13]:

• найнеобхідніша інформація міститься безпосередньо в пам'яті ІК, відповідним чином захищена і прямо використовується ІК-системою. Крім того, ІК є ключем для звернення до бази даних ІК-системи;

• база даних ІК-систем дублюють всю поточну інформацію ІК, її передісторію і містить ряд додаткових даних про кожен обслуговуваний об'єкт;

• ІК-технологія володіє ще однією цінною властивістю: ІК-системи легко інтегруються в складніші супер системи, яких теж може бути своя кількість рівнів, наприклад: системи префектури, міста, регіону, державна ІК-суперсистема.

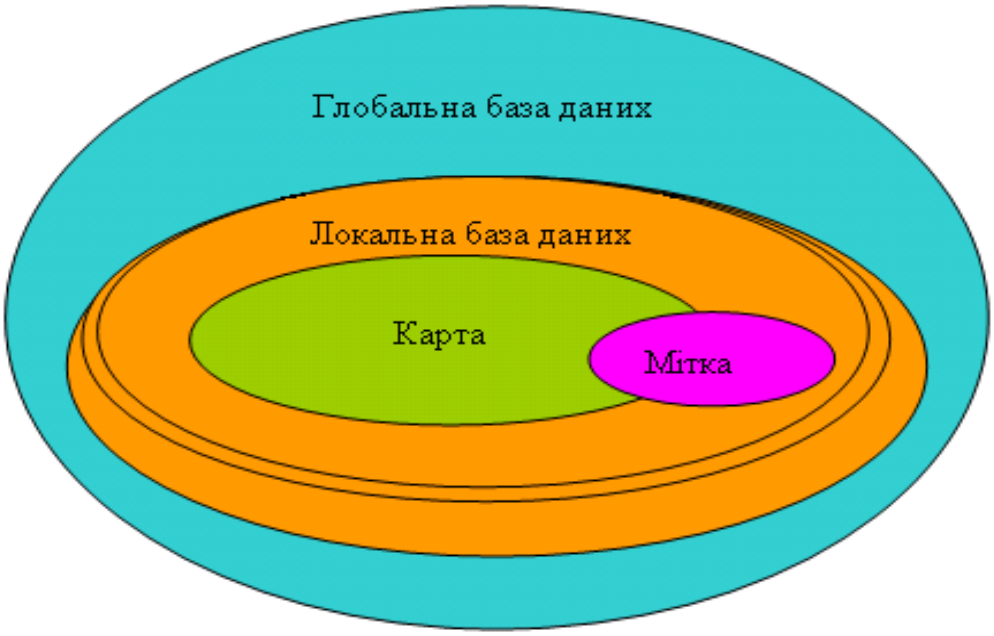

Рис. 2.2. Ієрархія баз даних ІК-систем

Тому, існує багато причин запровадження ІК. Більшість ІК включають у себе допоміжний реєстр, де і знаходиться така ж інформація, як і на картці.

Дивлячись на вигляд обслуговуваного об’єкта різноманітність ІК можна розділити на дві групи:

- ІК людини;
- ІК-документи;

- ІК матеріальних об'єктів: під об'єктом тут розуміється будь-яке устаткування, виріб, товар, тварина і все інше, причетне до процесу життєдіяльності людини і потреби індивідуального обслуговування для оптимізації цього процесу.

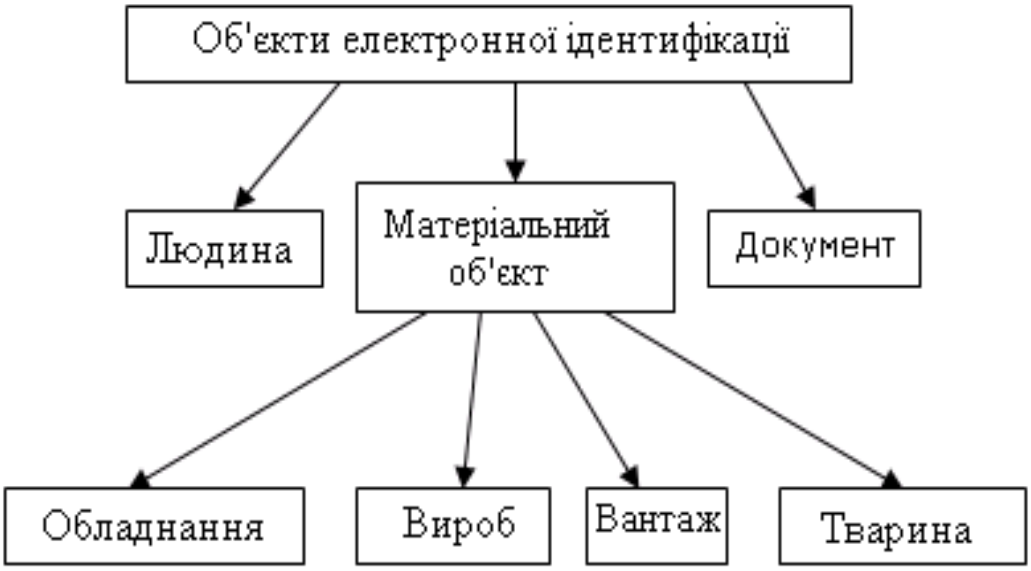

Рис. 2.3. Об'єкти ідентифікації

Можемо зробити висновок, що людина – це єдиний об'єкт, яка може пред'явити ІК і ІК його документів, які можуть як контактними, так і безконтактними. Всі інші документи завжди безконтактні.

Робоча частота визначає можливість і напрям бізнес-додатка RFID технології. Збільшено частоти RFID - технології розділяють на чотири діапазони:

- низькочастотний,
- високочастотний,
- надвисокочастотний
- мікрохвильовий (рис. 2.4) [9], [14], [15].

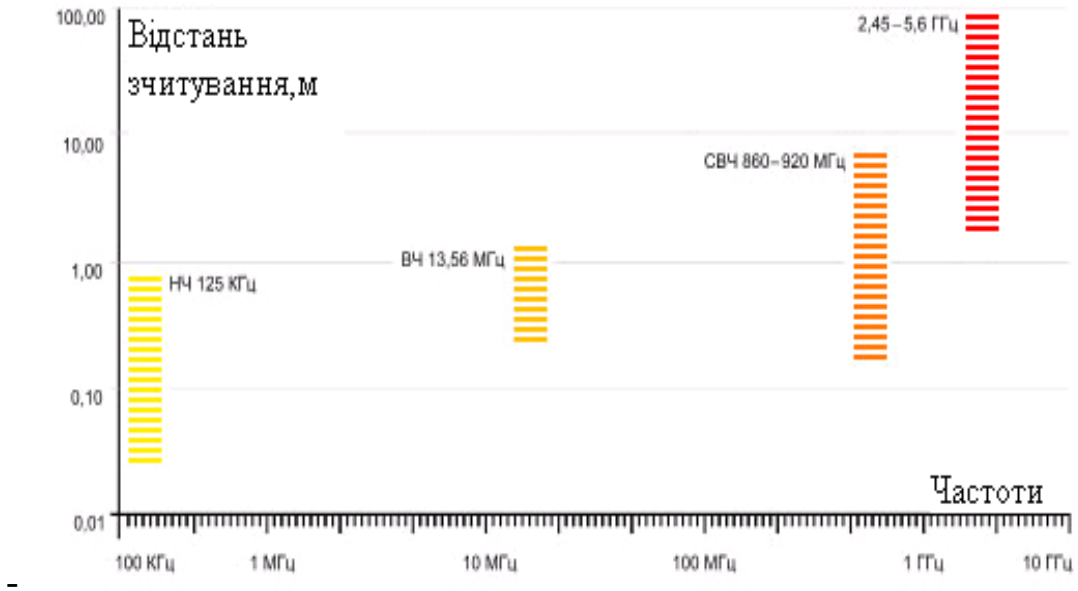

Рис. 2.4. Схематичне співвідношення частотних діапазонів і дальності зчитування у логарифмічних осях

Харатеристика чпстот.

Низькочастотний діапазон (Low frequency –LF).

Частоти: 125–134 КГц; (група стандартів ISO18000-2)

Дальність: 0,1–0,7 м-кодів ;

Сфера застосування: контроль доступу, автоіммобілайзер, ідентифікація тварин, промисловість, логістика.

Високочастотний діапазон (High frequency–HF).

Частоти: ~13,56 МГц; (ISO18000-3)

Дальність: 0,1–2 м-коди ;

Сфера застосування: логістика, контроль доступу, облік багажу, бібліотеки.

Надвисокочастотний діапазон (Ultra High frequency – UHF)

Частоти: 860 - 920 МГц; (стандарт ISO18000-6)

Дальність: 0,3–15 м-кодів;

Сфера застосування: логістика, промисловість, облік вантажів на транспорті.

Мікрохвильовий діапазон (Microvawe)

Частоти: 2,45. 5,6 ГГц; (ISO18000-4)

Дальність: 2–90 м-кодів ;

Сфера застосування: промисловість, ідентифікація транспорту

Високочастотні (13.56 МГц), які використовуються, там, де потрібно велика відстань та висока швидкість зчитування. Напикладі, контролю залізничних вагонів. Також, можемо побачити використання ридерів на шлагбаумі, а транспондер, який закріплюється на вітровому або бічному склі автомобіля. Даний діапазон частот використовує міжнародні стандарти. Це ISO 14443, ISO 15693, ISO 18000, EPC. Зазначимо, для ID документів, банківських і транспортних застосувань використовують ISO 14443. Сумісні з ISO 15683 і ISO 18000 систем - це VISINYTY системи, які застосовуються для маркування і обліку виробів на підприємстві в супермаркеті, для маркування і сортування багажу і поштових посилок і листів.

Проміжні частоти (10 МГц —15 МГц) використовуються, там де повинні передаватися великі кількості даних.

Низькочастотні (125-150 КГц). Можуть бути використані, там де невелика відстань між об’єктом і рідером. Більшість систем – це керування доступом, безконтактні картки, керування складом і виробництвом. Найчастіше використовують їх у вигляді карток або брелків.

Найбільш зручними у системах обліку системи діапазону UHF. В Україні UHF RFID використовуються з обмеженням у діапазоні 865-869 МГц.

На нашу думку, найбільш перспективним є стандарт UHF (868 МГц), тому що саме на цих частотах працюють безпровідні пристрої стандарту Bluetooth і Wi-Fi.

Стандарт DECT, в якого робоча частота міток і зчитувачів така, що не викликає збоїв у роботі комп’ютерів, мобільних телефонів.

Найсучаснішим і таким, який розвивається є стандарт UHF. Весь час з’являються мітки нової конструкції.

Загальні характеристики частотних діапазонів представлена у таблиці 1.

Таблиця 1

Загальні характеристики частотних діапазонів

Назва діапазону	**Робоча частота**	**Стандарт**	**Додатки**
Низькі частоти (LF)	125-150 КГц	ISO 14223 ISO 11784/11785 ISO 18000-2	Застосовуються в системах контролю доступу, для ідентифікації тварин, а також досить широкий використовуються, наприклад, в автомобільних іммобалайзерів
Високі частоти (HF)	13.56 Мгц	ISO 14443 ISO 15693 ISO 10373 ISO 18000-3	Застосовуються в системах контролю доступу, платіжних системах, а також для ідентифікації товарів в складських системах і книг в бібліотечних системах
Надвисокі частоти (UHF)	860-960 Мгц 2.4-5 Ггц	U-CODE 18000-4 18000-6	Сферою застосування є системи логістики і обліку руху транспорту. Відмітною особливість є підвищена дальність і висока швидкість читання

2.2. Технічна реалізація систем *радіочастотної ідентифікації*

Мітки (tag) RFID – пристрої, здатні зберігати і передавати дані. У пам'яті міток міститься їх унікальний ідентифікаційний код. Деякі мітки мають пам'ять, що перезаписується [15], [17].

Зчитувачі (reader) – прилади, які читають інформацію з міток і записують в них дані. Ці пристрої можуть бути як постійно підключеними до облікової системи, так і працювати за відсутності людини [15], [17].

Облікова система – програмне забезпечення, яке накопичує і аналізує отриману з міток інформацію і зв'язує всі елементи в єдину систему. Більшість сучасних облікових систем (програми сімейства 1С, корпоративні інформаційні системи – MS Axapta, R3Com) вже сумісні з RFID-технологією і не вимагають спеціального доопрацювання.

Схема функціонування RFID- системи представлена на рис. 2.5 [17].

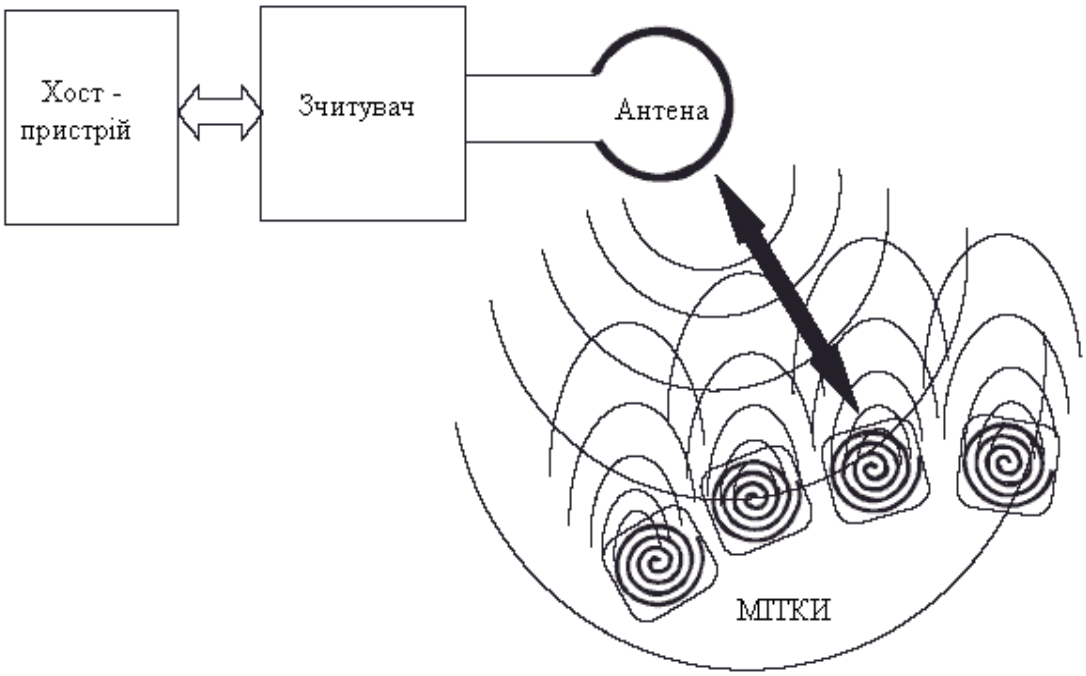

Рис. 2.5**.** Схема функціонування RFID- системи

В області ультрависоких частот (діапазон UHF - від 300 МГц до 3 ГГц) зв'язок між зчитувачем і міткою здійснюється за допомогою електромагнітних хвиль і дальність дії таких систем RFID (з пасивними мітками) зростає до одиниць метрів. Подальше підвищення дальності дії – до 10 - 100 метрів може бути досягнуте із застосуванням напівпасивних і активних міток (рис. 2.6).

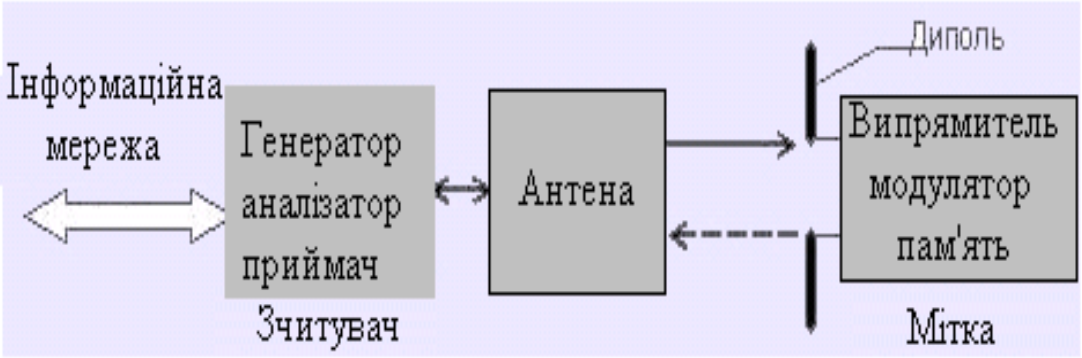

Рис. 2.6. Блок-схема системи RFID у діапазоні UHF з пасивною міткою

RFID-мітка інтегрує в єдину мікросхему – чіп. Який зберігає інформацію, і антени, за допомогою якої мітка ці дані передає і отримує. Індоі мітка можить мати власне джерело живлення(активна мітка), але більшість міток позбавлені їх (пасивні мітки).

Активні мітки використовують для передачі енергії власного елемента живлення. Дистанція таких міток може досягати 100 метрів.

Пасивні мітки використовують для передачі енергію поля зчитувача. Дистанція даних міток значно менша, і знаходиться в межах 0,05-8 метрів.

2.3. Типи існуючих RFID міток

Дана технологія використовується у будь-якому бізнесі. Саме її можна використовувати для збільшення прибутку та підвищення ефективності роботи.

Перевага її, полягає в тому, що не потрібно використовувати людський фактор у процесі ідентифікації.

Знаючи, які зчитувачі, де знаходяться, керівники компанії можуть відслідковувати – де знаходиться його товар, а також мати уявлення про переміщення продукції.

Для того, щоб системи, які засновані на даній технології були ефективні та працювали в будь-якому середовищу було розроблено RFID-мітки.

Їх розділяють за такими ознаками:

За типом живлення:

- активні – використовують для передачі даних енергію вбудованого елементу живлення (зона читання до 100 метрів).

- пасивні – використовують енергію, що випромінюється зчитувачем (дальність до 8 метрів) (Рис. 2.7., Рис. 2.8).

По видах пам'яті:

- "RO" (Read Only) – дані записуються лише один раз відразу при виготовленні. Такі мітки придатні для ідентифікації. Н нову інформацію у них записати не можна, і їх практично неможливо підробити.

- "WORM" (Write Once Read Many) – окрім унікального ідентифікатора такі мітки містять блок записуваної пам'яті, яку надалі можна багато разів читати.

- "RW" (Read and Write) – такі мітки містять ідентифікатор і блок пам'яті для зчитування/записи інформації. Дані в них можуть бути перезаписані велике число разів.

По виконанню (визначається цілями і умовами використання міток):

- паперові або лавсанові мітки;
- без клейового шару (інлайн або вставка);
- з клейовим шаром без поверхні для друку;
- з клейовим шаром і з поверхнею для друку;
- стандартні пластикові картки;
- дискові мітки (у тому числі з центральним отвором для закріплення на палеті);
- різні види брелоків;
- у спеціальному корпусі для особливих умов експлуатації.

Для будь-якого завдання можна підібрати відповідну мітку, яка буде спеціалізована до даної задачі.

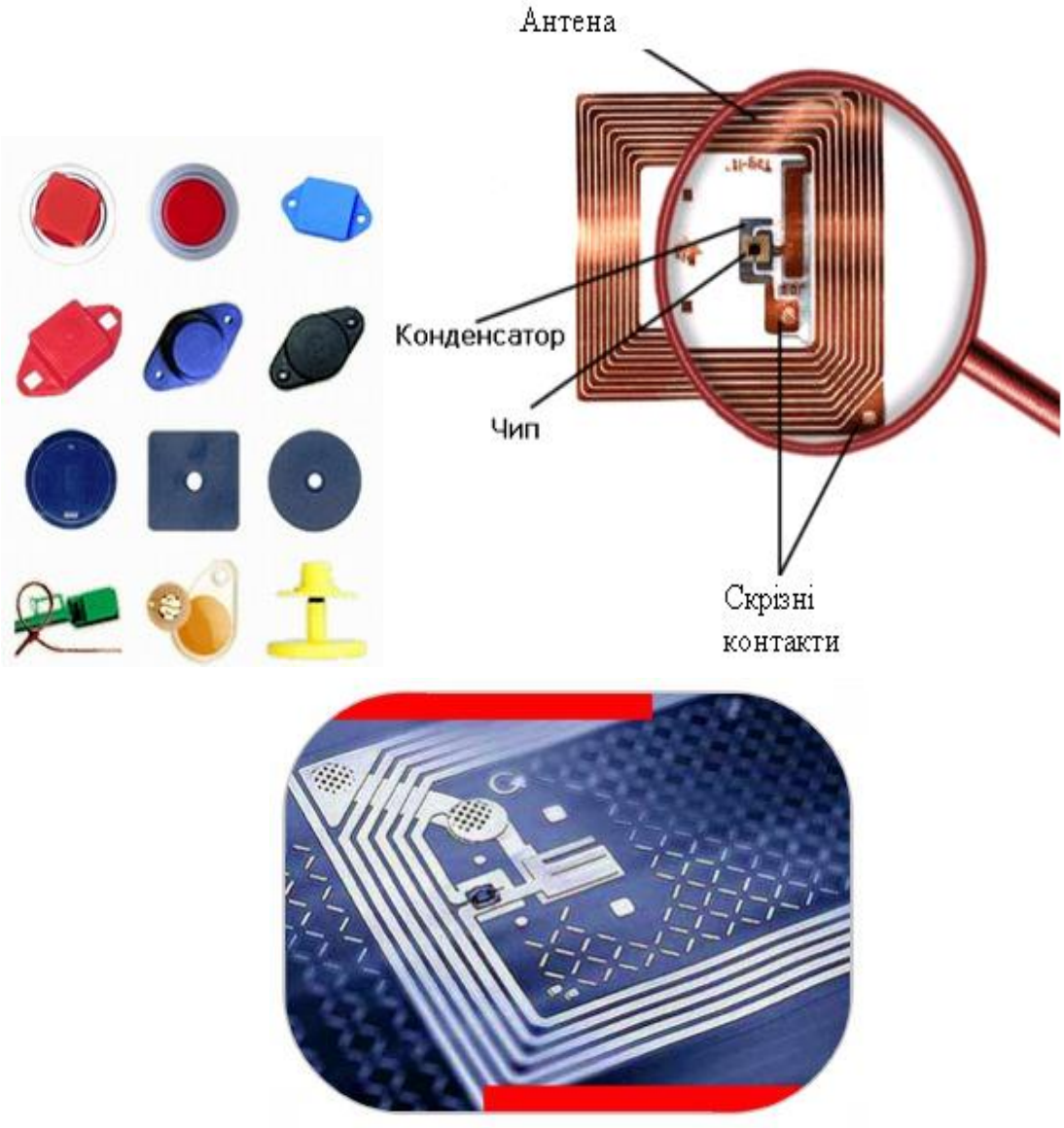

Рис. 2.7. Зовнішній вигляд пасивних міток

Рис. 2.8. СМАРТ - картка

2.4. Склад RFID міток

RFID – сучасна технологія автоматичної ідентифікації, саме вона дозволяє автоматизувати процес збору та обробку інформації безконтактним способом.

В даній технології, носієм інформації є радіохвиля. Для роботи не потрібно використовувати ні контакт зі зчитувачем, ні пряма видимість зчитувача. Однією з переваг є гарантована робота в агресивному середовищі та несприятливих кліматичних умовах.

RFID-мітка, складається з інтегрованої системи та антени. Мікрочіп зберігає інформацію, а антена передає та отримує сигнал. В свою чергу, антенна зчитувача випромінює електромагнітні хвилі, внаслідок цього і здійснюється живлення мітки. Результатом стає активування мітки та передавання інформації пристрою, що зчитується. Прямої видимості між зчитувачем та міткою не потрібно, що і допомагає легко проникати через більшість матеріалів. Тому, мітки повинні бути сховані усередині об’єктів, які підлягають ідентифікації.

Пам’ять RFID-міток містить їх унікальний ідентифікаційний код. Деякі з них мають перезаписувану пам’ять. Об’єм залежить від конкретної моделі чипа, більшість всього він не перевищує 2Кбіт. Одного з найбільшого поширення набули мітки з 96 бітами, які використовується лише для зберігання серійного номера партії або виробу. Також, існують мітки з об’ємом пам’яті до 4, 8, 32Кбайт. До них можна завантажувати дані, але і невеликі Java-додатки.

Зчитувач – це електронний пристрій, який зчитує інформацію з міток і записує у них дані. Ці пристрої можуть, як бути постійно підключеними до облікової системи, так і працювати автономно.

Облікова система – програмне забезпечення, яке накопичує та аналізує отриману з міток інформацію та пов’язує всі елементи в єдину систему.

Середня ціна за мітку все падає, і коли вона впаде нижче певної крапки, RFID буде готова вийти на мільярдний ринок логістики і скласти конкуренцію штрихкодам. Поки ж можна відзначити впровадження міток SmartCode у мережі міжнародних супермаркетів Wal-Mart, Targe, Tesco і Metro [11].

Потрібно відзначити появу стандартів EPC (electronic product code).

RFID можна побачити і в електронних документах. Якщо кредитна картка використовує чіп RFID, то на лицьовій стороні картки повинен бути зображений відповідний символ. Перші електронні паспорта були введені в Малайзії у 1998 році. А в 2003 році авіатранспортним комітетом Ради ICAO (Міжнародної Організації Цивільної Авіації) для забезпечення максимального рівня безпеки використання машинозчитувальних документів, що засвідчують особу в якості основи для нового стандарту, була схвалена рекомендація, щодо введення в дію паспортів, що містять електронні носії інформації.

При розробці сценаріїв закріплення міток на об’єкті потрібно враховувати, що зчитувачі оснащені антенами з лінійною поляризацією, що і і означає, що мітка розташована під одним кутом до антени, читатиметься на більшій відстані, чим при будь-якому розташуванні.

Орієнтувати мітку в просторі і добиватися прямої видимості не потрібно, тому що вона отримує енергію від поля, утворюваного антенами зчитувача. Варто зазначити, що RFID - зчитуватель може практично одночасно приймати інформацію відразу від декількох міток.

Деякі мітки необхідні для роботи протягом одного – двох тижнів, а інші супроводжуватимуть об’єкт роками. На даний момент існує велечезне різноманіття міток, тому відповідне виконання можна підібрати для будь-якого завдання.

Анти-коллизійне читання допомагає уникнути читання декількох міток одночасно, що знаходяться в зоні дії зчитувателя. У мітках попереднього покоління використовувалися анти-коллизіонні алгоритми на основі бінарного дерева, що не дозволяють швидко прочитувати велике число міток в зоні. Тому. Це обмежувало використання технології в реальних умовах.

Найбільш перспективними мітками є наступні:

- Пасивні (не вимагають живлення) мітки стандарту UHF, здатні працювати в умовах близькості до металу [17]. Не маючи вбудованого джерела живлення, використовують модуляцію віддзеркаленого сигналу. Внутрішня будова такого роду сенсорів складається лише із пластини, будь які активні електронні компоненти відсутні. Мітки такого стандарту коштують від 150 до 250 грн. Таким чином, подібні мітки виправдані для маркування дорогих об’єктів. Вони не задовольняються вимогам по мініатюрності і простоті розміщеності. Тому, розміщення подібних міток на деяких об’єктах обліку може бути утруднене або зовсім неможливе. Дані мітки дозволяють реалізувати і антикрадіжний захист.
- Мітки-наклейки. У випадках, коли скритно розташувати мітку неможливо (наприклад, відсутнє вільне місце корпусу, або корпус не можна розбирати, або розміри виробу менше розмірів самої мітки) доцільно застосовувати UHF мітки-наклейки на лавсановій або паперовій підкладці (рис. 2.9) [17].

Рис. 2.9. Мітка-наклейка

Дані мітки виграють за вартістю у порівнянні з попередніми, але програють по стійкості до механічних. Дистанція читання у них також нижча. Щоб ефективно працювати поблизу металу вони мають бути розміщення на зовнішніх поверхнях об’єкту, також можливо закріплювати і на внутрішній поверхні, якщо корус його виготовлений із пластика. При використанні даних

міток використовують моібльний зчитувач, який в порівнянні з іншими має меншу дальність дії і часто не має постійного зв’язку з програмою контролю та обліку. У мобільних зчитувачах є внутрішня пом’ять, в яку записують дані з проситаних міток.. Залежно від частоти діапазону мітки, дистанція стійкого зчитування і запису даних в них буде різна.

Антена є найважливішим елементом RFID – системи (рис. 2.10).

Рис. 2.10. Різномаїття антен

Антена випромінює електромагнітні хвилі, які і активізують RFID - мітку,які дозволяють проводити запис і зчитувати дані з цієї мітки. Саме вона є своєрідним каналом між міткою і приймачем, вона контролює весь процес і передачі даних. Антени можуть бути вбудовані в спеціальні сканери, ворота, одвірки для інформації від предметів або людей, що проходять через зону дії антени. Коли відбувається безперервне зчитування великої кількості міток, то електромагнітне поле випромінювання антеною постійне. Якщо постійне не потрібне, то поле може активуватися по команді оператора. Конструктивно антена і з декодером можуть знаходитися в одному корпусі. Функції і декодера схожі на функції аналогічних блоків в радіоприймачі і сканері. Сигнал, що з антени, демодулюється, розшифровується і передається через стандартний інтерфейс в комп'ютер для подальшої обробки [16].

Всі антени можна класифікувати (залежно від частоти) :

- по дальності дії (короткого, середнього і далекого радіусу)
- по виконанню (настільні, стаціонарні і портальні)
- по напряму поляризації (лівобічна, правобічна, двобічна)
- за швидкістю роботи (звичайні, швидкодіючі)

Елементи живлення у активних та пасивних мітках

Пасивні RFID-мітки не мають вбудованого джерела енергії. Комерційні реалізації низькочастотних RFID-міток можуть бути вбудовані в наклейку.

На даний момент, основна проблема RFID-пристроїв є те що для них потрібна зовнішня антена, яка за розміром перевищує чип. Кожна мітка має ідентифікаційний номер. Пасивні мітки можуть містити перезаписувану незалежні пам’ять. Наприклад, пасивні мітки Tag-it виробництва Texas Instruments мають FVW, що дозволяє користувачеві багато разів здійснювати перепрограмування сторіночок пам'яті [11].

Активні RFID-мітки володіють власним джерелом живлення і не залежать від енергії зчитувача, унаслідок чого вони читаються на дальній відстані, мають великі розміри і можуть бути оснащені додатковою електронікою. Такі мітки являються найдорожчими, а у батерей обмежений час роботи. Зате, саме вони в порівняні з попередніми є найдійнішими, завдяки особливій сесії зв’язку між мікою і пристроєм зчитування. Вони можуть генерувати вихідний сигнал більшого рівня, ніж пасивні, дозволяючи застосовувати їх в агресивніших для радіочастотного сигналу середовищах. Деякі RFID-мітки мають вбудовані сенсори, наприклад, для моніторингу температури товарів, які швидко псуються. Інші типи сенсорів в сукупності з активними мітками можуть застосовуватися для вимірювання вологості, реєстрації поштовхів/вібрації, світла, радіації, температури і газів в атмосфері (наприклад, етилену).

Також, ще однією перевагою активних міток є більший радіус зчитування і обсяг пам’ятів,, і здатні зберігати більший обсяг інформації для відправки приймачем.

Напівпасивні RFID-мітки, також їх називають напівактивними, дуже схожі на пасивні мітки, але оснащені батареєю, яка забезпечує чип енергоживленням. Дальність дії цих міток залежить тільки від чутливості

приймача зчитувача і функціонують на більшій відстані із кращими характеристиками.

Вартість міток визначається особливостями виконання кожного компонента. Від чого підвищується вартість? Основними ознаками, є:

- наявність елементу живлення;
- наявність перезаписуваної пам'яті великого об'єму (більше 2 Кбіт);
- стійкий до зовнішніх дій матеріал оболонки.

Прилади, які читають інформацію з міток і записують в них дані – зчитувачі. Вони можуть бути постійно підключеними до облікової системи, або працювати автономно. Залежно від частотного діапазону мітки, дистанція стійкого зчитування запису даних може бути різна. Розрізняють, як стаціонарні, так і мобільні.

Мобільні

Володіють меншою дальністю дії і часто не мають постійного зв’язку з програмою контролю обліку. Вони мають внутрішню пам’ять, в яку записують дані з прочитаних міток, і як стаціонарні зчитувачі здатні записувати дані в мітку (рис. 2.11).

До переносних належать ручні зчитувачі. Вони більш всього, поєднуються з терміналами збору даних. Менша дальність дії передбачена, тим що обмежена потужність джерела живлення. Ручні зчитувачі можуть записувати дані в мітку (інформація про проведення інформації).

Також з постійним розвитком технологій переважна більшість сучасних смартфонів оснащена NFS-модулем який може дуже легко виступати одночасно як RFID-карткою так і зчитувачем. Важливаю перевагаю такого застосування є додатковий захист у вигляді додаткової авторизації за допомогю Face ID або Touch ID , а також можливість зробити ключ який буде діяти лише обмежений період після верифікації що запобігає проникнення в систему методом копіювання RFID-сигналу зловмисниками оскільки скопійований ключ не буде діяти через короткий період часу після використання.

Рис. 2.11. Кишеньковий пристрій зчитування міток RFID і спеціальна рукавичка

Мобільні зчитувачі оснащені безпровідним зв’язком, забезпечують роботу в режимі реального часу (рис. 2.12).

Рис. 2.12. Мобільний зчитувач

Стаціонарні зчитувачі

Кріпляться нерухомо на стінах, порталах і в інших місцях (рис. 2.13. рис. 2.14) [9]. Також, можуть бути виконані у вигляді воріт, вмонтовані в стіл, або закріплені поряд з конвеєром на шляху проходження виробів. Зазвичай вони мають більшу зону читання і потужність, здатні одночасно обробляти дані з декількох десятків міток. Стаціонарні зчитувачі зазвичай підключені до комп’ютера, на якому встановлена програма контролю і обліку. Їх завдання полягає в поетапному фіксуванні переміщення маркованих об’єктів в реальному часі. Даний вид зчитувачу забезпечує максимально можливі

показники по дальності і швидкості дії. Ці зчитувачі можуть працювати з антенами різних типів.

Рис. 2.13. Настільний зчитувач для програмування міток

Рис. 2.14. Стаціонарні RFID-ворота

Мікросхема Intel для пристроїв зчитування RFID

Компанія Intel випустила мікросхему для реалізації на її базі зчитувача радіочастотних міток. Даний вид міток отримав назву Intel R1000 та орієнтований на модулях (Рис. 2.15) [10].

Рис. 2.15. Мікросхема Intel для пристроїв RFID

Саме Intel R1000 представляє велику інтегральну схему, яка об’єднує радіоприймальний тракт, блоки модуляції/демодуляції, процесор обробки сигналів, а також тракт UHF передавача.

Мікрочіпи компанії Hitachi

Компанія Hitachi створила найкомпактніший мікрочіп у світі. Саме він обіцяє стати технологічним проривом на ринку напівпровідників. Його розміри становлять 0,15 * 0,15 міліметрів і товщиною 7,5 мікрометрів, що є найкомпактнішим у світі. Зменшення габаритів досягнуто за допомогою розробленої японською компанією технології SOI. Настільки суттєве зменшення розмірів дозволить більш ніж у 4 рази збільшити продуктивність плат за рахунок можливості розташування на них більшої кількості чіпів. Нове покоління RFID чіпів від Hitachi цікаво тим, що володіє інтегрованою антеною (рис. 2.16) [10].

Даний чип може передавати 128-бітовий унікальний ідентифікаційний номер, записаний в мікросхему під час виробництва. Номер не можна бути зміненим надалі, що гарантує високий рівень достовірності і означає, що цей номер буде прив’язаний саме до того об’єкта, який приєднується або в який вбудовується цей чип.

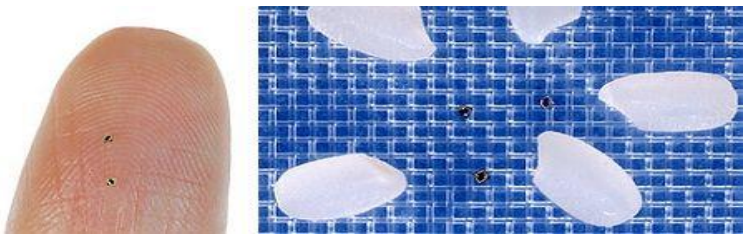

Рис. 2.16. RFID мікрочіп від Hitachi

2.5. Принцип роботи RFID міток

Найпростіші з міток являються транспондери. Вона являє собою LC контур. Зчитуючий пристрій складається з передавача і приймача (рис. 2.17) [17]. Коли транспондер потрапляє в зону дії антени передавального пристрою, він починаж генерувати і випромінювати через антену електромагнітні коливання, які уловлюються приймальною антеною, і система отримує повідомлення про присутність об’єкту в полі зчитування. Дані системи, можемо спостерігати в магазинах, супермаркетах і так далі. Такі транспондери виготовляються у вигляді етикетки, яка наклеюється на товар і в разі проносу товару поруч зі зчитувачем відбувається спрацювання сигналізації, що свідчить про крадіжку. Деактивація здійснюється шляхом руйнування LC контура.

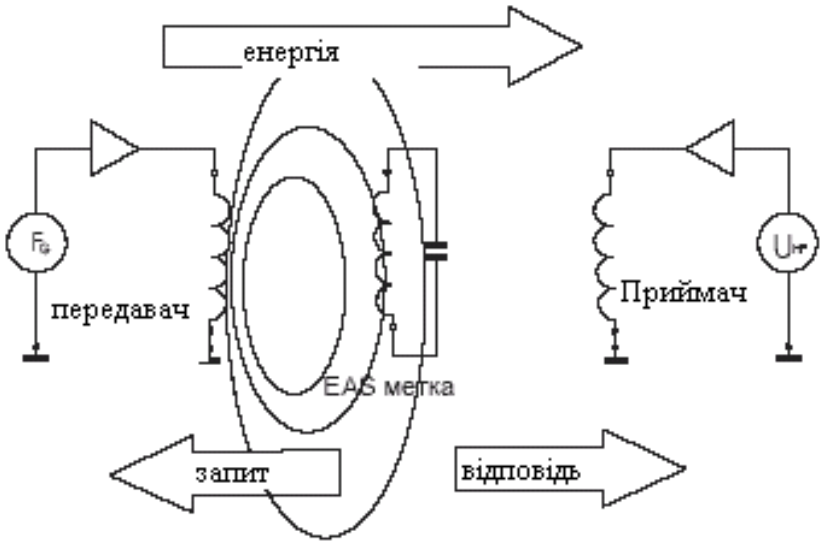

Рис. 2.17. Блок схема взаємодії

Описана система не дозволяє розрізняти об’єкти, бо вона здатна лише сповіщатипро факт її попадання в зону дії зчитувателя. Щоб ідентифікувати об’єкт кожен окремо, застосовуються мультимедійні транспондери. Мультібітний транспондером є пасивний з елементом пам'яті (рис.2.18).

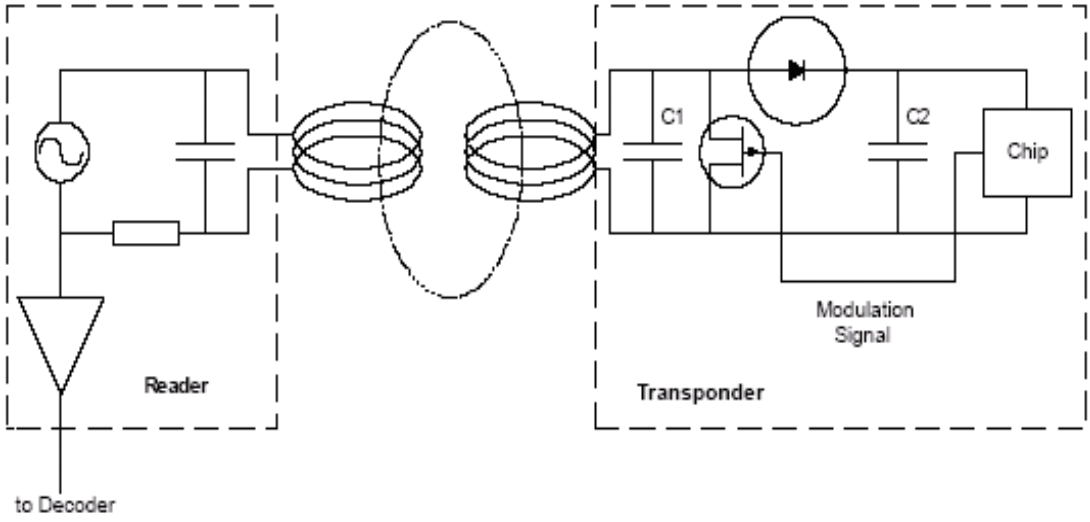

Рис. 2.18. Мультибітний транспондер

Найпростіший варіант це програмна пам’ять, в яку заноситься на заводі-виробнику унікальний серійниц номер UID. Мітка, потрапляючи в поле зчитувателя, отримує енергію, струм, наведений в антені транспондера, випрямляється і поступає на схему мітки, яка починає випромінювати коливання, які модулюються даними з пам'яті, і відбувається передача унікального серійного номера від мітки до зчитувателя [17].

Різноманітність міток є велика. Це мітки з можливістю лише зчитування з них інформації та складніші. Вони розрізняються за об’ємом пам’яті з різною організацією. Де необхідна підвищена захищеність передачі даних, використовується алгоритм криптозахисту. . У останніх поколіннях транспондерів застосовуються кристали, що несуть на своєму борту не лише незалежну пам'ять, а ще і мікропроцесор, що дає можливість транспондеру самому здійснювати необхідні обчислення і виконання алгоритмів (JAVA CARD) (рис. 2.19). Дані системи застосовують у банківських системах, електронні паспорти і так далі, де потрібна підвищена захищеність даних. А також, використання таких міток розвантажує система, що спрощує її як наслідок здешевлює.

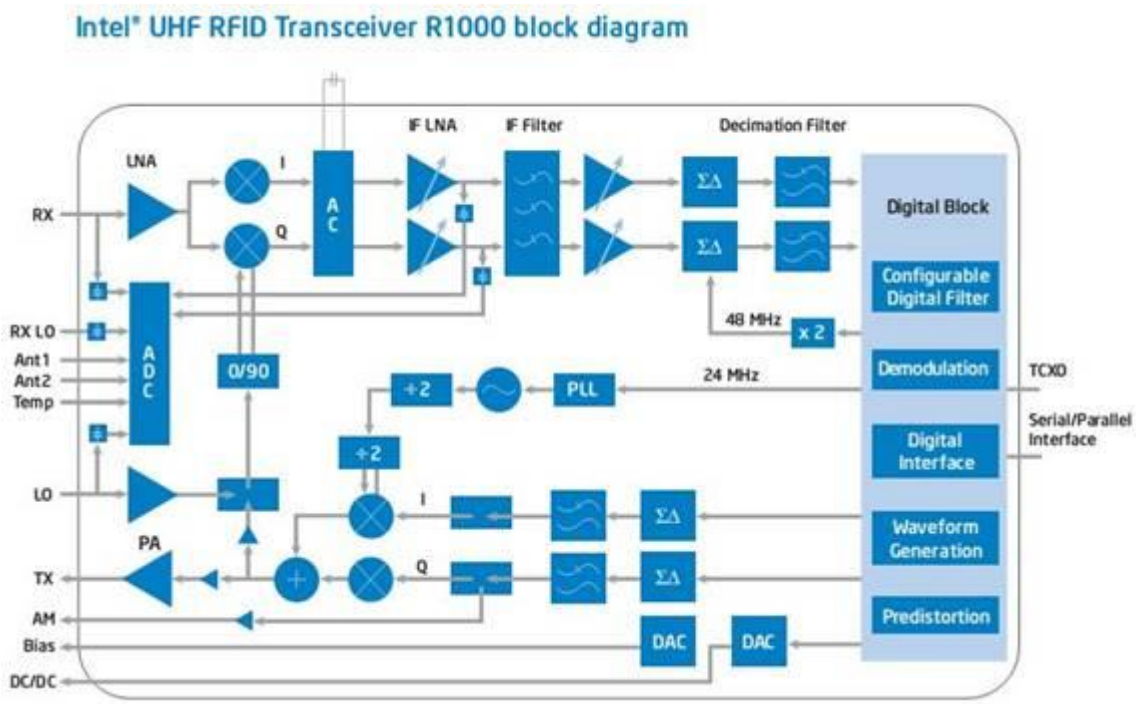

Рис. 2.19. Блок-схема мікрочипу Intel* UHF RFID Transceiver R1000

Технологія виробництва міток

Розглянемо виробництво на основі пластикових карток. Цикл виробництва мітки починається з виробництва кристала транспондера. Після цього, кристал кріпиться до антени, яка знаходиться на гнучкій пластиковій підкладці. Результатом є так званий інлей (від анг. Inlay) [103]. Далі інлей ламінується пластиком, і результатом є пластикова картка. Різноманіття форм представлена на зображенні (рис.2.20).

Рис. 2.20. Різномаїття форм транспондерів

Програма досліджень по технології виробництва міток є комплексною програмою, на розробку елементів систем радіочастотної ідентифікації (RFID) на базі тонких п'єзоелектричних плівок. Дані розробки створюються для

елементів нанопам'яті, наноелементів живлення, нанокомунікаторів і інших базових елементів RFID систем.

Мітки, побудовані за даною схемою володіють широким діапазоном робочих температур, які можуть працювати у несприятливих умовах (рис. 2.21).

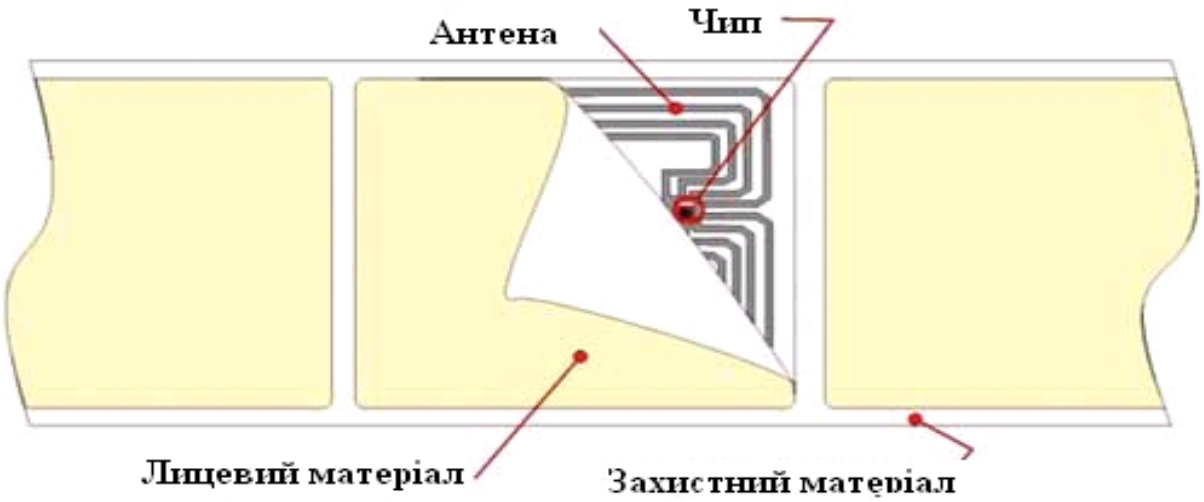

Рис. 2.21. Зовнішній вигляд розташування міток на стрічці

Особливості технології

- RFID-міткам не потрібен контакт або пряма видимість.
- Мітки читаються швидко і точно, які дозволяють виконати велику кількість сканувань.
- Мітки можна використовувати навіть в агресивних середовищах.
- Пасивні мітки мають фактично необмежений термін експлуатації.
- RFID-мітки можуть нести велику кількість інформації
- На невеликій відстанні можна відстежити мітки.
- Мітки можуть бути використанні як для читання, так і для запису великого обсягу інфорації.

2.6. Переваги та недоліки радіочастотної ідентифікації.

Переваги:

1. Можливість перезапису. Дані RFID-метки можуть перезаписуватися і доповнюватися багато раз, тоді як дані на штрих-коду не можуть бути змінені – вони записуються відразу при друці.
2. Відсутність необхідності в прямій видимості. RFID-рідеру не потрібна пряма видимість мітки, щоб рахувати її дані. Взаємна орієнтація мітки і зчитувача часто не грає ролі. Мітки можуть читатися через упаковку, що робить можливим їх приховане розміщення. Для читання даних мітці досить попасти в зону реєстрації, у тому числі при

переміщенні через неї на чималій швидкості. Навпаки, пристрою зчитування штрих-коду завжди необхідна пряма видимість штрих-коду для його читання.

3. Більша відстань читання. RFID-метка може прочитуватися на значно більшій відстані, чим штрих-код. Залежно від моделі мітки і зчитувача радіус зчитування може складати до декількох десятків метрів.

4. Більший об'єм зберігання даних. RFID-метка може зберігати значно більше інформації, ніж штрих-код. До 10000 байт можуть зберігатися на мікросхемі в 1 квадратний сантиметр, в той час, як штрихові коди можуть вміщати 100 байт (знаків) інформації, для відтворення яких знадобиться розмір з аркуш формату А4.

5. Підтримка читання декілька міток. Промислові рідери можуть одночасно прочитувати декілька десятків RFID-міток в секунду, використовуючи так звану антиколізійну функцію. Пристрій зчитування штрих кодів, проте, може одноразово сканувати лише один штрих-код.

6. Прочитування даних мітки при будь-якому її розташуванні. В цілях забезпечення автоматичного зчитування штрихового коду, комітетами із стандартів (у тому числі EAN International) розроблені правила розміщення штрих-міток на товарній і транспортній упаковці. До радіочастотних міток ці вимоги не відносяться. Єдина умова - знаходження мітки в зоні дії сканера.

7. Стійкість до дії довкілля. Існуючі RFID-метки володіють підвищеною міцністю і опірністю тяжким умовам робочої середи, а штрих-код легко ушкоджується (наприклад, вологою або забрудненням). У тих сферах, де один і той же об'єкт може використовуватися незлічену кількість разів (наприклад, при ідентифікації паллет або поворотної тари), радіочастотна мітка виявляється ідеальним засобом ідентифікації, так її не потрібно розміщувати на зовнішній стороні упаковки. Пасивні RFID-метки мають практично необмежений термін експлуатації.

8. Інтелектуальна поведінка. RFID-метка може використовуватися для виконання інших завдань, крім того, щоб бути просто охоронцем і переносником даних. Штрих-код же не володіє жодним інтелектом і є лише засобом зберігання даних.

9. Висока міра безпеки. Унікальне незмінне число-ідентифікатор, яке присвоюють мітці при виробництві, гарантує високу міру захисту міток від підробки. Також дані на мітці можуть бути зашифровані. Як і будь-який цифровий пристрій, радіочастотна мітка володіє можливістю закрити паролем операції запису і зчитування даних, а також зашифрувати їх. У одній мітці можна одночасно зберігати відкриті і закриті дані.

10. Пасивні мітки не мають батареї і фактично безсмертні.

Недоліки:

При роботі з радіочастотною ідентифікацією необхідно враховувати деякі обмеження. До них відносяться: відносно висока вартість; неможливість

розміщення під металевими і екрануючими поверхнями; взаємні колізії; схильність перешкодам у вигляді електромагнітних полів.

1. Відносно висока вартість міток. Вартість пасивної радіочастотної мітки складає від 0,15 долара (при придбанні понад 1 000 000 шт.) до 3 доларів (при придбанні 1 шт.). У випадку з мітками захищеного виконання (або на метал) ця ціна може досягати 7 і більш за долари. Таким чином, вартість RFID -меток перевищує вартість етикеток з штриховим кодом. Виходячи з цього, використання радіочастотних міток доцільне для захисту дорогих товарів від крадіжок або для забезпечення збереження виробів, переданих на гарантійне обслуговування. У сфері логістики і транспортування вантажів вартість радіочастотною виявляється абсолютно незначній в порівнянні з вартістю вмісту контейнера, тому абсолютно виправдано використання радіочастотних міток на пакувальних ящиках, палетах і контейнерах.
2. Можливе екранування при розміщенні на металевих поверхнях. Радіочастотні мітки схильні до впливу металу (це стосується упаковок певного вигляду - металевих контейнерів, інколи навіть деяких типів упаковки рідких харчових продуктів, запечатаних фольгою). Це зовсім не виключає вживання RFID, але приводить або до необхідності використання дорожчих міток, розроблених спеціально для установки на металеві поверхні або до нестандартних способів закріплення міток на об'єкті.
3. Схильність систем радіочастотної ідентифікації перешкодам у вигляді електромагнітних полів від ввімкненого устаткування, випромінюючого радіоперешкоди в діапазоні частот, який використовується для роботи RFID-системою. Необхідно ретельно проаналізувати умови, в яких система RFID експлуатуватиметься. Для систем UHF діапазону 868-869 МГц це практично не актуально (у цьому діапазоні жодні інші прилади не працюють), але низькочастотні мітки, що працюють на частоті 125 КГц до подібного впливу схильні.

Висновки до другого розділу

В данному розділи ми вивчили що таке RFID та RFID-мітки. Розібрали сутність технологію ознайомились з методами її реалізації. Оглянули типи міток та їх склад і які вони між собою відрізняються.

РОЗДІЛ 3. СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ З ВИКОРИСТАННЯМ RFID ТЕХНОЛОГІЙ

3.1. Методичні рекомендації щодо побудови системи захисту інформації на ОІД з використанням RFID технологій

На даний момент системи на базі технлогії радіочастотної ідентифікації отримали широке поширення, бо при мінмальних витратах дозволяють майже повністю автоматизувати контроль за місцезнаходженням об’єктів у приміщенях. Більш глобальні системи позиціонуються на базі супутникових та сотових технологій, які непридатні для вирішення даної задачі, бо їх застосування вимагає великих матеріальних витрат.

Рішення завдання моніторингу переміщення матеріальних носіїв з обмеженим доступом полягає в ому, що саме використовуються сучасні системи ідентифікації, що дозволяють здійснювати розпізнавання об’єктів на відстані до 100 метрів. Саме завдяки, таких ідентифікаторів і здійснюється контролювання матеріальних носіїв інформації у різних приміщеннях або різних підрозділах організації, і головним є те що система не потребує додаткових дій з боку співробітників. Ідентифікатори можуть бути виконані у вигляді міток-наклейок або корпусових міток.

На підприємствах, також можна використовувати ідентифікатори, що дозволяють здійснювати ідентифікацію зі значної відстані. Ідентифікатори підтримують стандарти proximity систем (Mifare, EM, HID),що дозволяє використовувати один і той же ідентифікатор для системи моніторингу і систем контролю доступу.

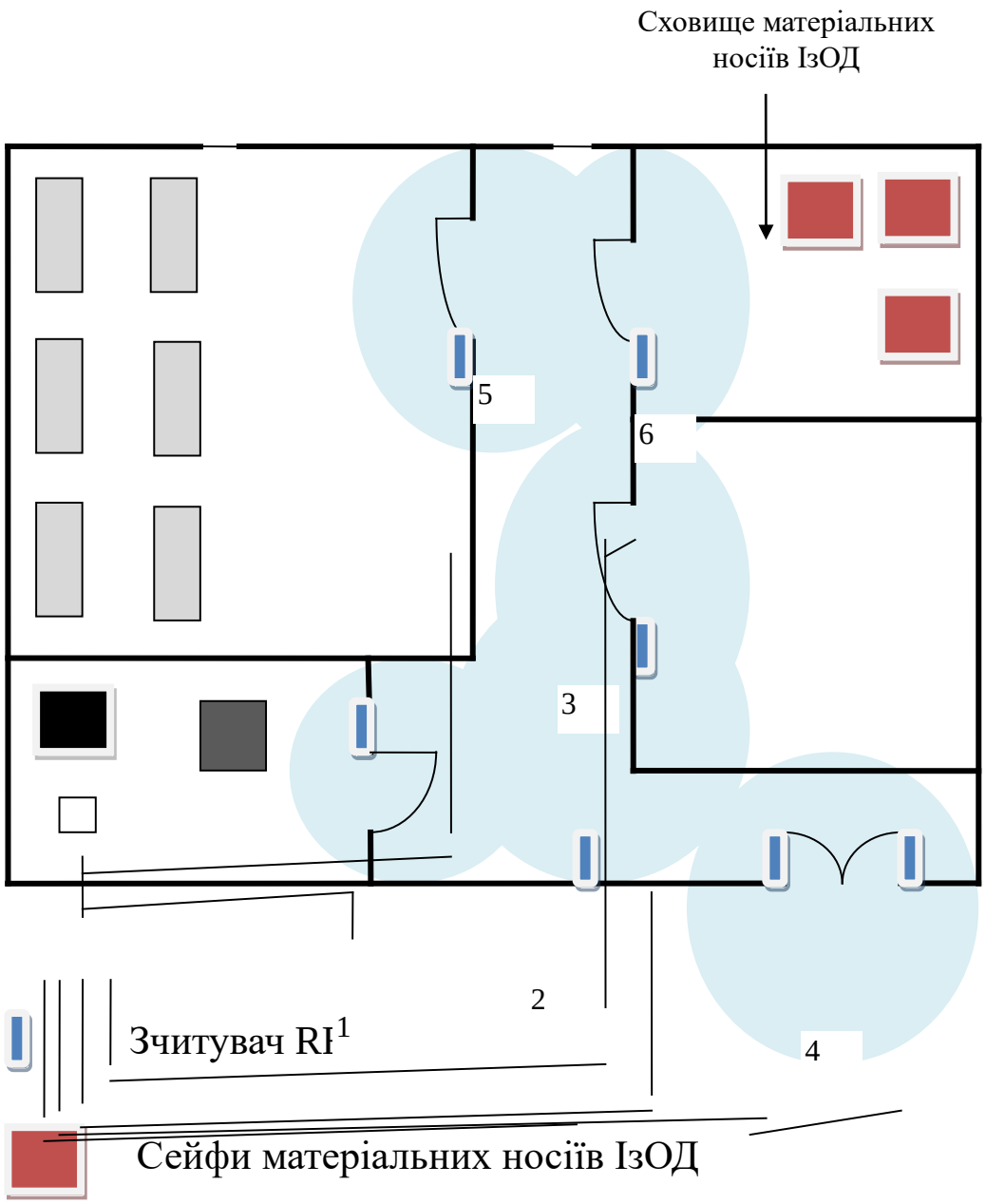
Сховище матеріальних носіїв ІзОД
5
6
3
2
4
Зчитувач RI[1]
Сейфи матеріальних носіїв ІзОД
Автоматизоване робоче місце чергової служби
Область дії RFID зчитувача

Рис.3.1. Варіант розміщення обладнання

Завдання, які допоможуть вирішувати системи, які побудовані на сучасному обладнанні радіочастотної ідентифікації для захисту інформації з обмеженим доступом від витоку матеріально-речовим каналом:

- Контроль часу знаходження матеріальних носіїв у певному місці;
- контроль місця знаходження матеріального носія з ІзОД;
- контроль знаходження матеріального носія з ІзОД на місці його зберігання;
- управління доступом у приміщення організації.

3.2. Методичні рекомендації щодо впровадження RFID-технологій

RFID-технологій мають широке поширення та впроваджуються в багатьох сферах. Наприклад, там де потрібна висока швидкість зчитування. Це використовується, для контролю автомобілів у русі, вагонів на залізниці. Високочастотні сканери монтуються у ворота або шлагбауми, а RFID-мітка встановлюється, наприклад на лобовому склі автомобіля. Дальність взаємодії мітки зі сканером становить від 4 до 8 метрів, що і створює переваги для людей, бо зчитувальний пристрій розташований поза межами їх досяжності.

Також, є популярний середньочастотний діапазон 10-15 МГц. Він використовуєтьбся в транспортних і аналогічних програмах.

Діапазон низьких частот 100-500 КГц діє на невеликій відстані між сканером і об’єктом.

Сферами застосування являються наступні:

- облік одиниць зберігання матеріальних носіїв ІзОД;
- формування топографії зберігання матеріальних носіїв ІзОД;

- автоматизація процесів пошуку примірників на місцях зберігання, проведення інвентаризації;
- відстеження та облік циркуляції і переміщення матеріальних носіїв ІзОД;
- обслуговування користувачів;
- забезпечення збереження матеріальних носіїв ІзОД, захист від несанкціонованого винесення і крадіжок, тобто витоку ІзОД матеріально-речовим каналом.

Переваги

- включення до складу облікової інформації додаткового (поряд з інвентарним номером) унікального коду, що дозволяє однозначно ідентифікувати кожен примірник носія в автоматизованому режимі, без звернення до інвентарних книгах, каталогах і картотеках;
- використання ідентифікаторів гарантованого рівня достовірності, тривалого терміну використання, значною механічної стійкості, розширеної функціональності в порівнянні з зі штрих-кодами або електромагнітними смугами;
- спрощення та збільшення швидкості видачі та прийому матеріальних носіїв ІзОД при проведенні обслуговування користувачів шляхом впровадження алгоритмів автоматизованої обробки даних та мінімізації процесів, що вимагають ручного введення інформації; основоположним перевагою RFID-технологій є можливість обробки декількох одиниць зберігання одноразово;
- забезпечення оперативного контролю наявності матеріальних носіїв ІзОД у сховищах, підсобних фондах, читальних залах, інших підрозділах та їх переміщеннях по території бібліотеки;
- можливість проведення інвентаризації бібліотечного фонду в автоматизованому режимі з мінімальними вимогами до дальності і площини розташування примірників видань, істотним зниженням застосування ручної праці і оперативним взаємодією з електронним каталогом (базами даних);

- захист матеріальних носіїв ІзОД від несанкціонованого переміщення за межі читацької зони та крадіжок;
- загальне скорочення кількості операцій на всіх етапах бібліотечних робіт: програмування читання / запису мітки в базі даних, оформлення видачі, здачі, продовження терміну користування, факту виявлення / не виявлення при інвентаризації і звірка з інформацією бази даних, активація / дезактивація анти-крадіжної функції здійснюється в межах однієї технологічної операції;
- максимальне скорочення тимчасових витрат на виконання стандартних операцій, скорочення ручної праці.

RFID-системи широко застосовуються. Типові застосовування:

- електронний контроль за доступом і переміщеннями персоналу на території підприємства;
- автоматизований збір даних і при необхідності нарухувати оплати на залізницях, платних автомобільних дорогах, на терміналах;
- громадський транспорт;
- системи електронних платежів для усіх видів транспорту;
- забезпечення безпеки (у комплексі з іншими технічними засобами аудіо- і відеоконтроль);
- захист і сигналізація на транспортних засобах;
- покращення логістики, зокрема на складах.

Кожна мітка має спеціальний сектор пам’яті, який зберігає унікальний ідентифікаційний код (ID) мітки - унікальний код, який фіксується в електронному каталозі АБИС поряд з інвентарним номером у складі облікових полів опису екземпляра.

Також, використовується при обслуговуванні користувачів, як основний ідентифікатор видаваного документа. Поряд із зберіганням ID-мітки в складі пам'яті присутній сектора пам'яті з можливістю запису і перезапису інформації, яка використовується для відміток про топографію зберігання даного примірника, а також активації або, навпаки, дезактивації протикрадіжного біта,

що відповідає відповідно позначці про дозвіл або заборону виносу видання з приміщення.

RFID-мітки зачасту використовуються в бібліотеках, що прискорює інвентаризацію і пошук книг,автоматизує книговидачу та допомагає боротися з крадіжками. Найбільша бібліотека, яка використовує RFID-мітки знаходиться у Ватикані, яка налічує в своєму фонді понад два мільйони примірників книг.

Для компакт-дисків, аудіо та відеокасет можливе застосування спеціалізованих міток (рис. 3.2).

Рис. 3.2. RFID-мітка для компакт диска

RFID-мітка практично необмежана терміном служби та не може бути підроблена, при штатному використанні; не вимагає оновлення; володіє функцію антиколлізії; володіє об’ємом пам’яті, яка достатня для забезпечення виконання всіх операцій з примірником протягом усьогоо його життєвого циклу.

Зчитувачі

Настільні зчитувачі

Застосовуються в бібліотеках, роздрібної торгівглі та багатьох інших областях. Яскравим прикладом є використання настільних зчитувачів у маркуванні шуб і хутряних виробів. Також, встановлюється в комплекті з плоскою настільної антеною і застосовуються у складі універсальних станцій програмування міток і станцій книговидачі (рис. 3.3, рис. 3.4 ,рис. 3.5):

Рис. 3.3. Зовнішній вигляд настільний зчитувача

Рис. 3.4. Зовнішній вигляд настільної антени

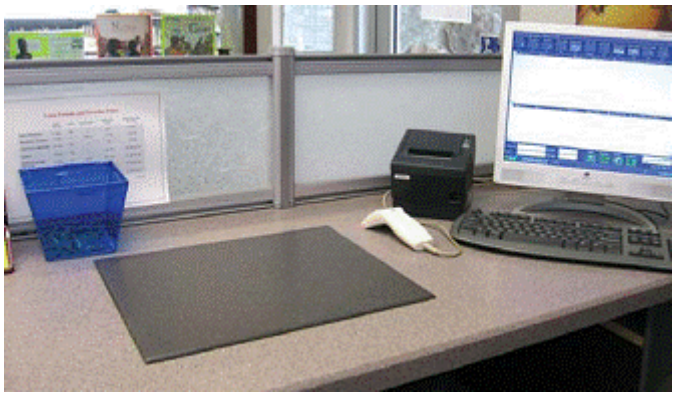

Рис. 3.5. Зовнішній вигляд автоматизованого робочого місця співробітника бібліотеки матеріальних носіїв ІзОД

Основними перевагами RFID спостерігається на етапі видачі матеріальних носіїв ІзОД та обслуговування користувачів. Зчитувач може сприймати кілька міток одночасно. Тому, відпадає необхідність підносити до зчитувача кожен видаваний документ.

Стаціонарні зчитувачі

Стаціонарні зчитувачі – прилад, змонтовані на різних пристроях, що застосовуються у сховищі матеріальних носіїв ІзОД.

Саме вони мають більшу зону читання і потужності, та здатні одночасно обробляти дані з декількох десятків міток. Зазвичай вони підключені до комп'ютера. Додатково можуть оснащуватися лічильником підрахунку.

Мобільні зчитувачі

Саме ці, зчитувачі використовуються в сховищах, підсобних і спеціалізованих фондах для швидкого пошуку та підбору потрібного видання на вимогу користувачів і тому подібних робіт.

Реалізація проєкту

Впровадження RFID-технологій у сховище матеріальних носіїв ІзОД включає у себе наступні етапи:

- широкомаштабне обстеження сховища:
  - параметри та характеристика будівлі;
  - організаційна структура бібліотеки;
  - об'ємні показники, склади, схеми розташування руху бібліотечного фонду;
  - системи обслуговування користувачів бібліотеки та активності використання, а також з урахуванням:
    - ✓ що використовується, та що планується до використання;
    - ✓ застосування автоматизованих бібліотечних технологій;
    - ✓ складу та обсягу електронних каталогів;
    - ✓ поставки, установки та тестування обладнання;
    - ✓ встановлення та налаштування обладнання;
    - ✓ навчання персоналу, методична та технічна підтримка;

ВИСНОВКИ ДО ТРЕТЬОГО РОЗДІЛУ

Розповіли детально про різні види зчитувачів та їх особливості і як вони можуть використовуватись в парі з мітками. А також надали рекомендації що до захисту матеріальних носіїв матеріально-технічним каналом.

Пропрацювали проект для провадження RFID-технології в роботу сховища матеріальних носіїв ІзОД. Він допоможе зробити роботу більш автоматизованою і організовано, а також дасть можливість розмежованого контролю доступу в приміщенні.

ВИСНОВКИ

1. Зараз безпека інформаційного простору має пріорітетне значення. Інформаційний світ розвивається надзвичайно швидко, а разом із ним розвивається попит на доступ до інформації з обмеженим доступом. Й тому для контр дії зловмисника постійно розвиваються методи захисту інформації. Для цього створюються служби безпеки, які контролюю вирішення інформаційних питаннь згідно норм, законів та вимог. На підприємствах утворються системи захисту інформації які складаються з фізичних та технічних елементів задля забезпечення повного контролю над інформацією.
2. У роботі досліджено технологію RFID, яка використовується у системах контролю та управління доступом і є дуже пошинерим та ефективним методом контролю. Розвиток радіочастотної ідентифікації показує що технологія дуже прогресивна і швидко розвивається, але потребує більше інвестицій.
3. Нами було розглянуто структуру, призначення, принципи, реалізації, а також переваги та недоліки різних RFID-міток. Зарахунок чого ми змогли зрозуміти в яких ситуаціях на краще використовувати окромі варіанти міток.
4. На основі дослідження була побудована система контролю матеріальних носіїв ІзОД у межах приміщення об’єкту інформаційної діяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України Про інформацію № 2657-XII від 2 жовтня 1992 року.
2. Закон України. Про державну таємницю. №1079-XIV 21 вересня 1999 року.
3. Закон України. Про захист інформації в інформаційно-комунікаційних системах № 1089-IX від 16.12.2020.
4. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
5. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
6. Козлов С.Б., Иванов Е.В. Предпринимательство и безопасность.- М.: Универсум, 1991.- Т1,2.
7. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации / Под ред. В.А. Хорошко. – К.: 2010. – Том I.
8. Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. Большая энциклопедия промышленного шпионажа.- СПб.: Полигон, 2000.-896с.
9. Ярочкин В.И. Информационная безопасность. Учебник для студентов ВУЗов. - М.: Академический Проект; Фонд «Мир», 2003.-640с.
10. В.Л. Джхунян, В.Ф. Шаньгин. Электронная идентификация. Бесконтактные идентификаторы и смарт карты. - М.: «Издательство АСТ»: Издательство «НТ Пресс», 2004.
11. K. Finkenzeller. RFID handbook: radiofrequency identification fundamentals and applications /Translated by R. Waddington/ J. Wiley & Son, Ltd, 2009.
12. R.A. Kleist, T.A. Chapmen et.al. RFID Labeling: Smart Labeling Concepts & Applications for the Consumer Packaged Goods Supply Chain/ Printronix, Inc., 2004.
13. Настільна книга по обмеженому доступу. Василенко Л.І.
14. Богуш В.М., Довидьков О.А. Теоретичні основи захищених інформаційних технологій - К.: ДУІКТ, 2006. – 508 С.

15. Гинце А. Новые технологии в СКУД // Системы безопасности, 2005. №6 Защита информации. Выпуск 1. М.: МП «Ирбис-11», 1992.
16. С. Черепков, «Стандарты и тенденции развития RFID-технологий», «Компоненты и технологи» № 1, 2006 р.
17. М. Федоров, «Технология RFID. Опыт использования и технологичне направления», «Компоненты и технологии» №9, 2005 р.
18. М.Гудін, В.Зайцев, «Устройства радиочастотной идентификации компании Tagsys», «Компоненты и технологии» №6, 2003 г.
19. Закон України «Про охорону праці». Введено в дію Постановою Верховної Ради України від 14.10.1992 г. № 2695 – XII.
20. Законодавство про охорону праці (основні положення).Методичний посібник. К., 1998
21. Жидецький «Основи охорони праці». Львів, 2000.
22. The Visual Microphone: Passive Recovery of Sound from Video. Abe Davis