

2. Барсенгян А.А. Анализ данных и процессов. – 3-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2009. – 512 с.: ил.

**Диесперов А.В.**

*студент;*

**Яшков И.О.**

*кандидат технических наук, доцент,*

*Харьковский национальный университет радиоэлектроники*

## **ОСОБЕННОСТИ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПРИ ПОМОЩИ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ**

Сегодня система контроля востребована в предприятиях и деловых центрах. Она выполняет ряд задач: предотвращает проникновение посторонних лиц на территорию, ведёт их учёт на вход и выход. Преимущество автоматизированного контроля – отсутствие человеческого фактора. В данной работе будут рассматриваться электронные замки с использованием электронных ключей.

Электронный замок – электронное устройство, предназначенное для того, чтобы предотвратить доступ в помещение посторонних лиц, или наоборот, ограничить выход из помещения. Решение о доступе лиц в помещение принимается на основе сигналов от различных датчиков: считывателей магнитных карт, штрих-кодов, датчиков контактной памяти, биометрических датчиков, наборной клавиатуры, дистанционного управления и т.д. Часто является частью сложной электронной системы контроля доступа, иногда неотделим от нее. В качестве исполнительных механизмов используются электромеханические и электромагнитные запорные устройства.

Электронный ключ – портативное устройство для отпирания двери с электронным замком, выполненное в виде магнитной карточки, бесконтактного устройства, действующего на некотором расстоянии, или устройства с электрическим контактом.

Преимущество электронных замков – это возможность предоставления доступа одновременно нескольким личностям, не требует замены в случае утери всех ключей. Рассмотрим типы ключей:

### **1. Магнитная карта**

Магнитная карта – это пластиковая карта, которая соответствует спецификациям ISO, имеет на обратной стороне магнитную полосу с информацией объемом около 100 байт памяти, которая считывается специальным считывающим устройством, и место для подписи. Такие магнитные карточки широко используются во всем мире как банковские кредитные и дебетовые карты. Магнитная полоса может быть изготовлена для различных мощностей магнитного поля, и по этому параметру различают высококоэрцитивную (HiCo) и

низкокоэрцитивную (LoCo). Степень коэрцитивности влияет на устойчивость записанной информации к размагничиванию. Пластиковые карты с магнитной полосой HiCo более надежны и долговечны, так как информация на магнитных полосах HiCo менее подвержена размагничиванию внешними магнитными полями, чем на полосах LoCo.

## 2. Бесконтактные ключи

Чтобы открыть замок вам не придется вынимать и прикладывать свой ключ к считывающему устройству, нужно просто приблизиться на достаточно близкое расстояние и замок откроется.

Вдаваясь в подробности, считыватель замка постоянно излучает магнитное поле, попадая в которое чип бесконтактного ключа активируется и посылает свой код в считывающее устройство. В следствии чего – срабатывает замок.

Для примера более детально рассмотрим устройство бесконтактного брелока-заготовки RFID 125, которая имеет чип производства США, рабочую частоту 125 кГц и ряд усовершенствованных аналогов. Данная модель может быть перепрограммирована бесконечное количество раз, а также финализована.

## 3. Ключи с электрическим контактом.

Данный вид ключей содержит электро-схему, которая передаёт приёмнику (замку) цифровой ключ в виде цифрового сигнала, где происходит сравнение ключа на устройстве с ключом в базе. Этот вид ключа можно поделить на программируемый и непрограммируемый вид. Ключи могут выпускаться с прошитым внутри ключом, или программируемым одноразово или многократно.

Помимо преимуществ электронных ключей, они имеют некоторые недостатки. При несложной конструкции – легко подделать или взломать. Для более высокой безопасности требуется более сложная конструкция устройства и ПО.

Использование «электронных ключей» в будущем актуально, но до тех пор, пока не будут разработаны и широко внедрены биологические системы безопасности. Самый универсальный способ – это электронный ключ с программируемым чипом. Возможность его использования не ограничено: в интеллектуальном доме, на предприятии, при доступе к различным электронным устройствам и т.д.

### **Список использованных источников:**

1. Комплексные системы безопасности, 2015 – Режим доступа: <http://системы-безопасности.com.ua/>
2. Свободная энциклопедия, 2016 – Режим доступа: <https://wikipedia.org>
3. Платежные системы, 2016 – Режим доступа: <http://dengi.polnaya.info/>
4. Изготовление ключей, 2015 – Режим доступа: <http://key-smt.com.ua/>