

# Турникеты систем контроля и управления доступом и применяющиеся в них методы идентификации

Олег Харламов

Турникеты давно стали частью автоматизированных систем контроля и управления доступом. В современных системах контроля доступа турникеты оснащаются различными биометрическими средствами идентификации. В статье рассматриваются недостатки подобных средств и приводится пример перспективной российской разработки – автоматизированной системы контроля и управления доступом (АСКУД) на базе шлюзового турникета с мультимодальной биометрической идентификацией и аутентификацией.

## Термины и определения

Система контроля и управления доступом, СКУД (англ. Physical Access Control System, PACS) – совокупность программно-аппаратных технических средств безопасности, имеющих целью ограничение и регистрацию входа-выхода объектов (людей, транспорта) на заданной территории через точки прохода: двери, ворота, турникеты, КПП.

Основная задача СКУД – управление доступом на заданную территорию (кого пускать, в какое время и на какую территорию), включая:

- ограничение доступа на заданную территорию;
- идентификацию лица/объекта, имеющего доступ на заданную территорию.

Турникет (фр. *tourniquet*) – устройство, предназначенное для физического ограничения прохода людей в случае, когда необходима проверка права входа и выхода для каждого проходящего.

## Виды турникетов СКУД

В зависимости от назначения турникеты различаются по своей конструкции, материалам, структуре, степени защиты, пропускной способности, принципу действия и пр. По виду управления турникеты бывают полностью автоматическими, с ручным управлением (посредством оператора), а также со смешанными режимами.

Выделяют следующие базовые конструктивы турникетов СКУД:

- калитки;
- триподы;
- роторные;
- створчатые;
- шлюзовые.

## Турникет-калитка

На рис. 1 приведён пример турникета типа калитка. Это недорогой, малогабаритный и простой в эксплуатации турникет. Он состоит из опорной стойки и открывающейся створки. Сама створка может быть различной по размерам, конструкции и материалам. Управление данным турникетом может осуществляться оборудованием системы контроля доступа, с пульта управления, в автоматическом режиме (например, только на выход или вход, как в супермаркете).

## Трипод

Трипод – наиболее простая конструкция турникета. Препяжающую функцию выполняют три планки, установленные на барабане под углом к оси его вращения и под углом 120 градусов друг к другу, при этом одна из трёх планок всегда находится в положении, параллельном земле, препятствуя проходу, а остальные планки находятся в положениях, не препятствующих проходу. На рис. 2 представлен пример турникета данного типа. Проходящий через турникет человек толкает планку, препятствующую проходу, это вынуждает барабан провернуться, и планка оказывается за

пределами прохода, в то время как её место занимает следующая, препятствуя проходу следующему человеку.

Тумбовый трипод – это трипод, установленный в уже сформированном проходе. По принципу работы аналогичен триподу, однако отличается более

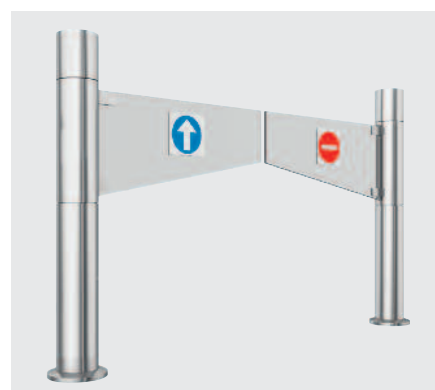


Рис. 1. Турникет-калитка



Рис. 2. Турникет-трипод



Рис. 3. Турникет-трипод тумбовый

высокой степенью защищённости (его сложнее обойти). Пример такого решения показан на рис. 3.

### Роторный турникет

Конструкция роторного турникета (рис. 4) представляет собой вертикальную ось, обладающую вращающимися лопастями. Лопасти устройства могут быть выполнены из различных материалов. Существуют варианты, где лопасти изготовлены из параллельно расположенных штанг. Такая система подходит для помещений, отличающихся высокими показателями проходимости. В сравнении с триподами роторный турникет требует больше свободной площади. Встречаются полнопрофильные и полупрофильные исполнения.

### Створчатый турникет

В данном виде турникетов (рис. 5) в качестве преграждающего устройства применяются створки, управляемые электроприводами. Этот вид турникетов оснащается необходимым набором датчиков, позволяющих исполнительному механизму получить информацию о подходе человека к турникету и о проходе через него, а также служащих для предотвращения прохода нескольких человек одновременно. Например, турникеты данного типа установлены в метрополитене.

### Шлюзовой турникет

На рис. 6 представлен пример шлюзового турникета створчатого типа. Данный конструктив отличается наиболее высокой степенью защиты, а при необходимости возможна блокировка нарушителя. Существуют исполнения, конструктивно близкие как к роторным, так и к створчатым турникетам (в последнем случае добавляется второй ряд створок – выходных). Шлюзовой турникет преимущественно устанавливается на объектах с высокими и очень



Рис. 4. Роторный турникет

высокими требованиями к безопасности. Он может быть оборудован различными датчиками, вплоть до детекторов следов взрывчатых веществ, ядерных материалов и др. Конструкция турникета отличается высокой надёжностью, работает в различных температурных диапазонах. Возможны исполнения для ответственных применений и жёстких условий эксплуатации.

## ОСНОВНЫЕ МЕТОДЫ ИДЕНТИФИКАЦИИ СКУД

ГОСТ Р 51241-98 определяет термин «идентификация» как процесс опознавания субъекта или объекта по присущему или присвоенному ему идентификационному признаку. Под идентификацией понимается и присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов, то есть процесс идентификации рассматривается как сравнение введённого в систему идентификационного признака (кода) с образцами кодов, хранящимися в памяти системы (поиск и сравнение одного со многими).

Следует обратить внимание на термин «аутентификация» – это процедура проверки подлинности введённых



Рис. 5. Створчатый турникет

субъектом идентификационных данных с эталоном (образом), хранящимся в памяти системы для данного субъекта (процесс аутентификации рассматривается как сравнение одного с одним).

Данные понятия близки по смыслу и часто используются не только в области контроля доступа. Рассмотрим основные методы идентификации и аутентификации в СКУД и их слабые стороны.

### Идентификация по запоминаемому коду

Очевидный недостаток метода – то, что зачастую код записывают на бумаге и хранят её в доступном для потенциального нарушителя месте. При большом потоке людей ошибки, связанные с неправильным набором кода, резко снижают пропускную способность. Сами считыватели недостаточно защищены от манипуляций (наблюдение, подбор).

### Идентификация по вещественному коду

Наиболее очевидный недостаток – идентификатор (предмет, RFID-метка) может быть украден, скопирован, утерян или даже преднамеренно передан постороннему лицу.



Рис. 6. Шлюзовой турникет

## Биометрическая идентификация

Поскольку при использовании описанных методов идентификации в СКУД не существует принципиальной защиты от ряда рисков, то это в целом существенно снижает уровень защищённости охраняемого объекта. Как следствие производители турникетов стали расширять модельные ряды, дополняя свою продукцию средствами биометрической идентификации. В настоящее время существует множество статических методов (основываются на физиологической статической характеристике человека, которая не меняется в течение довольно длительного времени) биометрической идентификации. К наиболее известным можно отнести методы, основанные на использовании таких характеристик, как:

- отпечаток пальца;
- форма (геометрия) лица;
- подкожный рисунок вен ладони;
- сетчатка глаза;
- радужная оболочка глаза;
- геометрия кисти руки;
- ДНК.

В силу высокой стоимости технологии и значительного времени проведения

идентификации в системах управления доступом из перечисленного наиболее часто можно встретить методы биометрической идентификации, основанные на использовании перечисленных далее характеристик.

### 1. Отпечаток пальца

*Основные недостатки:*

- папиллярный узор отпечатка пальца легко повреждается (вследствие травмы или определённой профессиональной деятельности);
- сканеры требуют регулярной очистки поверхности;
- технология контактная – возникают вопросы гигиены;
- недостаточная защищённость от подделки изображения отпечатка.

### 2. Форма (геометрия) лица

*Основные недостатки:*

- форма 2D: низкая статистическая достоверность, наличие определённых требований к освещению, неприемлемость каких-либо внешних помех (например, очки, борода, некоторые элементы причёски);
- форма 3D: дороговизна оборудования (превосходит по цене даже сканеры радужной оболочки), измене-

ния мимики лица и помехи на лице ухудшают статистическую надёжность метода.

### 3. Подкожный рисунок вен ладони

*Основные недостатки:*

- недопустима засветка сканера солнечными лучами и лучами галогенных ламп;
- некоторые возрастные заболевания, например артрит, ухудшают статистические результаты работы алгоритма.

### 4. Сетчатка глаза

*Основные недостатки:*

- сложная в использовании система с высоким временем обработки;
- высокая стоимость системы;
- отсутствие широкого рынка и, как следствие, недостаточная интенсивность развития метода;
- опасения пользователей, связанные с возможными повреждениями глаз.

### 5. Радужная оболочка глаза

*Основные недостатки:*

- стоимость системы, основанной на идентификации по радужной оболочке, выше стоимости системы, основанной на распознавании отпечатка пальца или лица;

**LUMINEO**  
POWERED BY ВЕПЕО

**ДИСПЛЕИ ДЛЯ**  
**от -50°C**

**PROSOFT®**  
WWW.PROSOFT.RU

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

- низкая доступность готовых решений на рынке;
- опасения пользователей, связанные с возможными повреждениями глаз.

Вне зависимости от категории методов идентификации каждый из них по отдельности имеет свой ряд различных по степени существенности недостатков. На данном фоне особо перспективными выглядят мультимодальные системы, то есть те, которые используют комбинацию двух и более методов идентификации, что значительно повышает уровень достоверности идентификации, упрощает процедуру прохода для субъектов, а при определённых конфигурациях и существенно сокращает время проведения процедуры идентификации.

### ПРИМЕР РЕАЛИЗАЦИИ

В качестве примера рассмотрим более подробно одну из интересных российских разработок, использующую мультимодальную идентификацию, – шлюзовой турникет с применением двухфакторной биометрической идентификации: по подкожному рисунку вен ладоней и видеораспознаванию лиц. Общий вид системы турникетов показан на рис. 7.



Рис. 7. Общий вид трёх проходов АСКУД

Данная автоматизированная система контроля и управления доступом (АСКУД) представляет собой совокупность аппаратных и программных компонентов, связанных между собой и готовых для интеграции в инфраструктуру пункта контроля. Система является новым шагом в оптимизации алгоритмов пропуска людей в закрытые зоны. Шлюзовой турникет был разработан российской компанией ПРОСОФТ и её технологическими партнёрами. В полностью

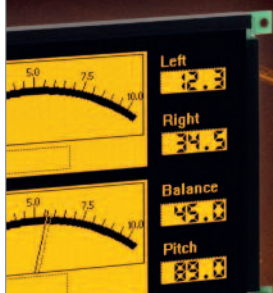
автоматизированном режиме система выполняет функции идентификации личности и принятия решения о непосредственном пропуске субъектов в закрытый периметр.

Система поддерживает основные операционные функции контроля:

- идентификация личности по биометрическим/персональным данным;
- аутентификация личности по биометрическим данным с использованием установочных данных;

## ЖЁСТКИХ УСЛОВИЙ

до +85°C



### Основные свойства электролюминесцентных дисплеев

- Кристальная чёткость изображения. Отсутствует размытость изображения движущегося объекта при температуре  $-60^{\circ}\text{C}$
- Широкий угол обзора – свыше  $160^{\circ}$
- Время отклика менее 1 мс
- Средний срок безотказной работы более 116 000 часов
- Срок эксплуатации не менее 11 лет при потере яркости 25–30%
- Устойчивость к ударным и вибрационным воздействиям
- Низкий уровень электромагнитного излучения
- Компактный корпус и обрамление

### Области применения

- Специальная техника
- Транспортные средства
- Промышленное оборудование
- Медицинские приборы
- Аппаратура морской техники

**LUMINEO**  
POWERED BY ВЕРТЕQ

МОСКВА  
(495) 234-0636  
info@prosoft.ru

САНКТ-ПЕТЕРБУРГ  
(812) 448-0444  
info@spb.prosoft.ru

ЕКАТЕРИНБУРГ  
(343) 356-5111  
info@prosoftsystems.ru



Рис. 8

- контроль по спискам оперативного учёта лиц и другим источникам.

Дизайн – стоечные конструкции, соединённые прозрачными стенками. Конструкция АСКУД формирует коридор для передвижения человека. Двери и боковые стенки образуют безопасный шлюз, всё пространство шлюза полностью просматривается, обеспечивая максимальный обзор и контроль действий человека. Внешние компоненты АСКУД обеспечивают антивандальные принципы защиты. Это относится ко всем компонентам и деталям АСКУД, с которыми может контактировать человек. Случайные удары, прикосновения и иные действия не способны причинить значительный вред конструкции и привести к нарушению работы комплекса.

Модульность конструкции АСКУД обеспечивает масштабируемость и позволяет снять ограничения на число отдельных АСКУД или групп АСКУД при организации линий прохода.

Все компоненты обеспечивают удобство для человека при прохождении через АСКУД, для этого конструктив включает информационные экраны, свето-

диодные сигналы, аудиоустройства оповещения и связи с диспетчером.

Архитектура АСКУД включает следующие механизмы контроля:

- контроль нахождения и направление движения человека при подходе к АСКУД, при выполнении процедур биометрического сканирования, при движении человека в АСКУД во время открытия входных дверей;
- контроль движения входных и выходных дверей для того, чтобы человек не был защемлён и не осуществлялось блокирование движения дверей;
- контроль нахождения только одного человека в шлюзе АСКУД;
- интеллектуальное видеонаблюдение за действиями человека (контроль оставленных предметов, нештатное поведение человека, попытки покинуть шлюз непредусмотренным способом или перекинуть какие-либо предметы и т.п.).

В зависимости от потребностей возможна реализация любого сценария прохода и применение любой комбинации механизмов идентификации:

- RFID-метки;
- распознавание лиц;

- верификация информации по носителям, содержащим биометрическую информацию;
- распознавание отпечатков пальцев;
- распознавание рисунка вен ладоней.

При необходимости возможно применение системы распознавания голоса и других методов.

Конструкция АСКУД обеспечивает быструю установку на любую поверхность, легко перемещается и не вызывает проблем при замене или добавлении новых компонентов с течением времени, в том числе и при увеличении количества линий контроля.

Конструктивное исполнение АСКУД предусматривает в период эксплуатации замену (добавление) узлов и блоков с учётом прогнозируемого развития аппаратных и программных средств:

- замену узлов и блоков с меньшим сроком службы (средств вычислительной техники, считывателей и других элементов и механизмов);
- добавление, модификацию считывателей новых биометрических параметров;
- замену блоков технологической конструкции АСКУД с учётом возмож-

**swissbit®**  
INDUSTRIAL MEMORY SOLUTIONS



## Серия S-40: карты памяти SD и MicroSD для эффективных промышленных применений

- 4–32 Гбайт (MLC NAND Flash)
- SD 3.0 (2.0), SDHC Class 6
- Передача данных до 24 Мбайт/с
- Автономная система управления данными
- Защита от пропадаания напряжения
- Длительное время хранения данных при экстремальных температурах
- Резервирование встроенного программного обеспечения
- Сложный механизм распределения нагрузки и управления сбойными блоками
- Обновление параметров и встроенного программного обеспечения
- Контроль изменений в комплектации
- Инструменты для диагностики

**Надёжные, прочные,  
экономичные**

**PROSOFT®**

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

(495) 234-0636  
INFO@PROSOFT.RU

[WWW.PROSOFT.RU](http://WWW.PROSOFT.RU)



Реклама

ных изменений в технологической схеме или для модернизации;

- замену других узлов и блоков с учётом прогнозируемого развития аппаратно-программных средств.

Рассмотрим некоторые примеры сценариев прохода.

#### **Одновременное применение сканера рисунка вен ладоней и видеораспознавания лица**

На первом этапе субъект, желающий попасть в закрытую зону, должен пройти процедуру идентификации, а именно на входе в шлюзовой турникет необходимо приложить ладонь к биометрическому сканеру рисунка вен. Если идентификация прошла успешно, система открывает створки шлюза и впускает человека внутрь шлюза в зону аутентификации. После попадания субъекта внутрь шлюза, входные створки закрываются. Внутри шлюза находится камера, выполняющая поиск и фотографирование лица субъекта для проведения процедуры аутентификации личности. С целью оптимизации алгоритмов поиска лица камера имеет возможность автоматически изменять своё положение. По результатам выполнения процедур идентификации и аутентификации система принимает решение об открытии выходных створок и пропуске субъекта в закрытую зону.

#### **Применение сканера носителя биометрической информации и видеораспознавания лица**

Сначала субъект, желающий попасть в закрытую зону, должен пройти процедуру идентификации — на входе в шлюзовой турникет необходимо приложить к сканеру соответствующий носитель биометрической информации. Если идентификация прошла успешно, система открывает створки шлюза и впускает субъекта внутрь шлюза в зону аутентификации. После попадания человека внутрь шлюза входные створки закрываются. Внутри шлюза находится камера, выполняющая поиск и фотографирование лица субъекта для проведения процедуры аутентификации личности путём сравнения полученного изображения с образцом, считанным с носителя биометрической информации. С целью оптимизации алгоритмов поиска лица камера имеет возможность автоматически изменять своё положение. По результатам выполнения процедур идентификации и аутентификации система принимает решение об открытии выходных створок и пропуске субъекта в закрытую зону.

#### **Применение сканера RFID-метки и биометрического сканера рисунка вен ладони**

В данном сценарии субъект, желающий попасть в закрытую зону, должен пройти процедуру идентификации, а именно на входе в шлюзовой турникет необходимо приложить к сканеру носитель, содержащий RFID-метку. Если идентификация прошла успешно, система открывает створки шлюза и впускает человека внутрь шлюза в зону аутентификации. После попадания субъекта внутрь шлюза, входные створки закрываются. Внутри шлюза находится биометрический сканер рисунка вен. Человеку необходимо приложить к нему ладонь для проведения процедуры аутентификации личности. По результатам выполнения процедур идентификации и аутентификации система принимает решение об открытии выходных створок и пропуске субъекта в закрытую зону.

Конструктив приведённой в качестве примера системы достаточно универсален. Система способна настраиваться

на индивидуальные потребности заказчиков, как с точки зрения функциональности, так и с точки зрения внешнего дизайна и конструктива. Данное решение востребовано на объектах, предъявляющих повышенные требования к контролю доступа, таких как специализированные пропускные пункты, банковские и музейные хранилища, склады особо ценных изделий и опасных веществ, объекты с критической инфраструктурой и другие.

#### **ЗАКЛЮЧЕНИЕ**

Комбинаций методов идентификации и аутентификации много, так же как и конструктивов самих турникетов. Всё зависит от назначения системы и потребностей заказчика. Остальное — это вопросы законодательной применимости методов и специфики технической реализации конкретного решения. ●

**Автор – сотрудник  
фирмы ПРОСОФТ  
Телефон: (495) 234-0636  
E-mail: info@prosoft.ru**

## НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

### **Модуль MAQ<sup>®</sup>20 от Dataforth заслужил почётное звание «Выбор инженеров 2018 года»**

Модуль MAQ20-DODC20SK производства компании Dataforth был удостоен почётного звания Engineers' Choice Award («Выбор инженеров») журнала Control Engineering в номинации «Аппаратное обеспечение для сбора данных».

Представленный впервые в феврале 2017 года дискретный выходной модуль DODC20SK высокой плотности имеет 20 изолированных выходов, предназначенных для коммутации сигналов до 60 В при 3 А постоянного тока. Выходные параметры модуля по умолчанию настраиваются пользователем, и каналы можно коммутировать по отдельности или в блочном формате. Пользователь может определить стандартную или инвертированную логическую полярность. Присоединение модуля осуществляется посредством пружинных клеммных колодок высокой плотности, облегчающих и ускоряющих подключение. Среди других параметров MAQ20-DODC20SK можно отметить изоляцию между выходными каналами и шиной до 1500 В и перегрузочную способность канала по напряжению (в случае непреднамеренных ошибок подключения) до 60 В постоянного тока. Допустимый потенциал между каналами 150 В позволяет модулю управлять оборудованием с общим сигналь-



ным заземлением или без него, а также устройствами с разными опорными потенциалами.

Как и все модули семейства MAQ20, MAQ20-DODC20SK предназначен для установки в опасных зонах класса I, подкласса 2 и обладает высокой помехоустойчивостью, обычно необходимой в тяжёлых промышленных условиях.

— Мы гордимся тем, что продукция компании Dataforth удостоена почётного звания Engineers' Choice Award, — заявил менеджер по продажам и маркетингу компании Dataforth Георг Хаубнер. — Выдающиеся характеристики модуля MAQ20-DODC20SK значительно расширяют общие возможности и гибкость системы MAQ20, а теперь мы получили официальное признание этого. ●