Анализ подходов к разработке системы контроля и управления доступом предприятия

А. Б. Мудрич, К. В. Ежова

***Аннотация*—В статье рассматривается концептуальный подход к разработке системы контроля и управления доступом (СКУД) предприятия на основе применения технологий биометрии.**

Одной из важнейших задач любой организации является поддержание высокого уровня безопасности, что может быть достигнуто за счет внедрения на территории предприятия охранно-пропускных систем различного уровня сложности. В представленной работе особое внимание уделяется принципам разработки систем видеонаблюдения с функцией распознавания лиц. Как правило, такие системы представляют собой сложный аппаратно-программный комплекс с функцией детектирования и распознавания объектов на основе алгоритмов компьютерного зрения. При этом к системам безопасности данного класса предъявляется ряд жестких требований как на уровне аппаратного обеспечения, так и на уровне программной реализации. Для камер видеонаблюдения такими требованиями являются их технические характеристики, которые должны обеспечить достаточно высокое качество передаваемого видеопотока для задач последующего распознавания объектов на нем. Для программного обеспечения – это необходимое быстродействие для работы в режиме реального времени и требуемая точность алгоритмов идентификации.

В первом разделе рассматривается понятие системы контроля и управления доступом. Во втором разделе – основные требования к системам видеонаблюдения, осуществляющим распознавание объектов. Третий раздел содержит описание концепции разрабатываемой системы и перспектив ее дальнейшего развития в рамках научно-инженерной работы.

***Ключевые слова* — система контроля и управления доступом (СКУД), распознавание лиц, система видеонаблюдения, система безопасности.**

I. Введение

Для любого предприятия (организации) вопросы безопасности собственных сотрудников, объектов, территории и интеллектуальной собственности имеют первостепенный характер. Нарушения в данной сфере могут привести не только к финансовым потерям, но и к репутационным рискам со стороны организации в случае кражи интеллектуальной собственности.

Основной системой, отвечающей за обеспечение безопасности и организацию контрольно-пропускного режима на территории организации, является система контроля и управления доступом (далее по тексту сокр. – СКУД) [1]. СКУД может быть организована различным образом и обладать разной степенью автоматизации – от простого КПП с турникетом до сложной автоматизированной системы, реализованной на аппаратном и программном уровне [2].

На данный момент на рынке системы контроля и управления доступом представлены достаточно широко, но при этом можно отметить ряд проблем существующих систем, среди которых:

1) отсутствие комплексного решения, способного выполнять все функции СКУД – учет и хранение данных о допусках сотрудников и внешних посетителей, обеспечение идентификации посетителей, предупреждение о несанкционированном доступе в помещения и др.;
2) существующие решения, предполагающие использование функций интеллектуального видеонаблюдения, сложны в настройке и управлении для рядового сотрудника поста охраны;
3) дорогое обслуживание, в том числе включая сопровождение со стороны компании-разработчика;
4) неточность и проблемы в применяемых алгоритмах распознавания;
5) сложность масштабирования – расширения и настройки системы на новом объекте (сильная зависимость от инфраструктуры предприятия) и др.

Необходимость решения перечисленных проблем говорит о потенциале развития рынка систем безопасности, включая СКУД, и возможности создания собственного продукта, который будет востребован на рынке информационных систем безопасности и сможет решить часть описанных проблем.

II. Понятие системы контроля и управления доступом (СКУД)

A. Понятие и функции СКУД

Под СКУД понимается аппаратно-программный комплекс, устройства которого должны препятствовать несанкционированному доступу на территорию предприятия (турникеты, пропускные устройства и др.), фиксировать его (камеры, датчики движения и др.) и сообщать о нем (различные сигнальные системы), и программные средства для работы перечисленных устройств (драйверы) и взаимодействия с пользователем

Статья получена 31 октября 2022.

Мудрич Анна Бобановна, Университет ИТМО (mudrich_ab@niuitmo.ru).

Ежова Ксения Викторовна, Университет ИТМО (ezhovakv@itmo.ru).

(интерфейс, база данных и др.) [3].

Основные функции систем контроля и управления доступом: санкционирование, идентификация, авторизация, аутентификация, разрешение или отказ в доступе, регистрация и реагирование [4].

Важным компонентом в работе СКУД является возможность организации контрольно-пропускного режима предприятия (КПР), в основе работы которого лежит механизм «запретов» и «ограничений» по отношению к лицам, попадающим на территорию организации [5]. Особый контрольно-пропускной режим можно установить как для всей организации, так и для ее отдельных компонентов (помещений). Это позволяет назначить разным объектам (помещениям) в границах одного предприятия различные уровни допуска [6]. Существование дифференциации помещений по степени закрытости для посетителей разных категорий (уровней допуска) является важным аспектом при проектировании СКУД в целом и политики уровней безопасности для разных пользователей (посетителей) в частности.

B. Компоненты СКУД

Независимо от специфики реализации системы контроля и управления доступом на конкретном предприятия, любая СКУД будет состоять из перечисленных ниже компонентов (рис. 1) [7]:

Рис 1. Общая схема СКУД [7]

Идентификатор пользователя – это устройство или признак, по которому можно провести однозначную идентификацию посетителя. Идентификаторы можно разделить на атрибутные и биометрические. Примерами атрибутивных идентификаторов являются электронные пропуски, токены, примерами биометрических – лицо, голос и другие биологические атрибуты пользователя системы.

Устройство идентификации личности (считыватель) – устройство, которое осуществляет считывание идентификатора пользователя и передает полученные данные на контроллер. Примерами считывателей является кнопочная клавиатура для ввода кода доступа, считыватель карт, биометрический считыватель и др.

Контроллер обрабатывает информацию от считывателя идентификаторов и на основе полученных данных управляет исполнительным устройством (разрешение или запрет на проход через КПП).

Исполнительное устройство представляет собой механизм, который физически ограничивает доступ на территорию объекта: турникет, замок, автоматические ворота и др. Открытие исполнительного устройства осуществляет контроллер при получении корректного идентификатора личности пользователя.

К описанной выше структуре в первую очередь стоит обращаться на начальных этапах проектирования СКУД - на этапах определения аппаратной базы и выбора технологий проектирования и разработки программно-информационной подсистемы. Разрабатываемая система планируется как биометрическая СКУД, поэтому в качестве основных элементов выступят следующие компоненты:

1) идентификатор пользователя – биометрические данные (лицо посетителя);
2) устройство идентификации – камера видеонаблюдения, размещенная в помещении, или специальный биометрический датчик на КПП;
3) контроллер – зависит от реализованной в организации пропускной системы;
4) исполнительное устройство – турникет на входе в офис или цифровой замок на двери помещения.

Дополнительно в случае реализации только подсистемы видеонаблюдения (подробнее концепция системы будет описана в последнем разделе) с функцией идентификации посетителей на месте контроллера и исполнительного устройства будет находиться клиентское приложение, осуществляющее получение данных с видеокамер, выполнение идентификации и передачу информации на интерфейс пользователя.

III. Системы видеонаблюдения с функцией детекции и распознавания объектов

Как упоминалось выше, СКУД представляет собой аппаратно-программный комплекс, основной функцией которого является предотвращение и информирование о несанкционированном доступе на территорию организации[3]. Таким образом, важным этапом проектирования любой системы контроля и управления доступом является правильный выбор соответствующего задачам и архитектуре системы оборудования.

Для представленной автоматизированной системы основными аппаратными компонентами будут выступать камеры видеонаблюдения. Откуда возникает необходимость более подробного анализа доступных на рынке камер и их ключевых характеристик.

По способу передачи и обработки сигнала все камеры можно разделить на аналоговые и цифровые [8]. В аналоговых камерах изображение с камер передается в виде аналогового сигнала, который отцифровывается для обработки, но для передачи снова преобразуется в исходный аналоговый сигнал. Принцип обработки изображения в аналоговой камере представлен на рис. 2 [9].

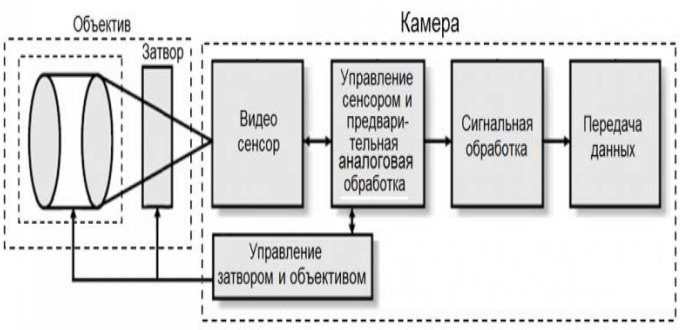

Рис 2. Принцип обработки изображения в аналоговой камере[9]

В цифровых камерах передача и обработка сигнала происходит полностью в цифровом формате. При этом сигнал может передаваться как в исходном виде – HDI-SDкамеры [10], так и сжиматься и кодироваться для увеличения скорости передачи данных (например, IP-камеры [11]). Процесс передачи и обработки сигнала в цифровой камере представлен на рисунке ниже (рис. 3) [12].

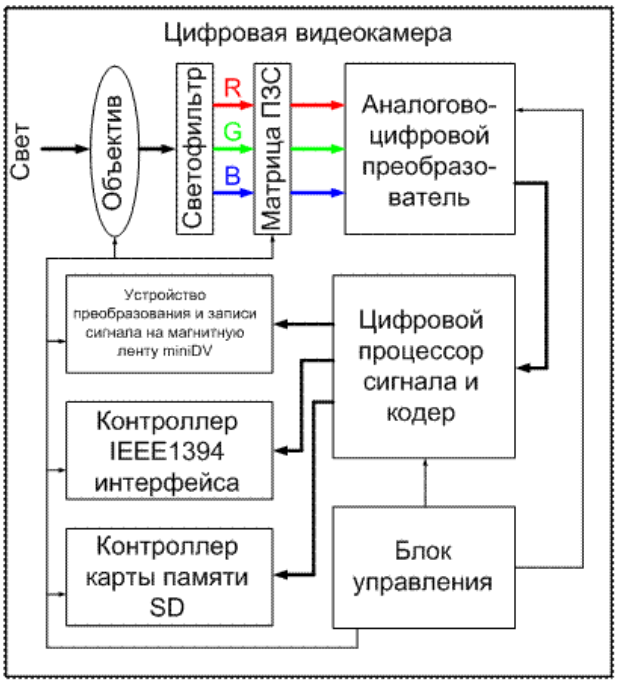

Рис 3. Принцип обработки изображения в цифровой камере[12]

Важным требованием к камерам, задействованным в системах видеонаблюдения с реализованной функцией распознавания лиц, является высокое качество получаемого изображения. Рекомендуемое качество видео в таких системах должно быть не ниже 720 px [13]. Основным недостатком аналоговых камер и аналоговой передачи сигнала является низкое качество получаемого изображения (особенно для старых моделей), поэтому в системах с распознаванием лиц чаще используются современные цифровые камеры с высоким качеством изображения.

Помимо типа передаваемого сигнала (аналоговый или цифровой) важной характеристикой при выборе камер для систем видеонаблюдения с распознаванием лиц являются угол обзора. Он определяется размером матрицы и фокусным расстоянием [14].

Говоря о фокусном расстоянии камеры, в первую очередь, имеется в виду заднее фокусное расстояние (f') – в первом приближении его можно определить, как расстояние от поверхности последней линзы объектива камеры до точки заднего фокуса [15]. От фокусного расстояния обратно пропорционально зависит угол обзора камеры, который рассчитывается по формуле [14]:

$$\alpha = 2\text{arctg}(d/2f) \quad (1)$$

где α - угол обзора камеры,
d – размер светочувствительности сенсора,
f' – фокусное расстояние.

По данной формуле, исходя из характеристик конкретной камеры и дистанций обнаружения и распознавания объекта для конкретного помещения, можно подобрать подходящую камеру.

Ниже представлена приблизительная зависимость угла обзора от фокусного расстояния камеры (рис. 4) [13]:

Фокусное расстояние	2,8мм	3,6мм	6мм	8мм	12мм	16мм
Угол обзора	86°	72°	48°	30°	25°	17°
Расстояние до объекта	0- 5м	0- 6м	5- 10м	10- 20м	25- 35м	35- 50м

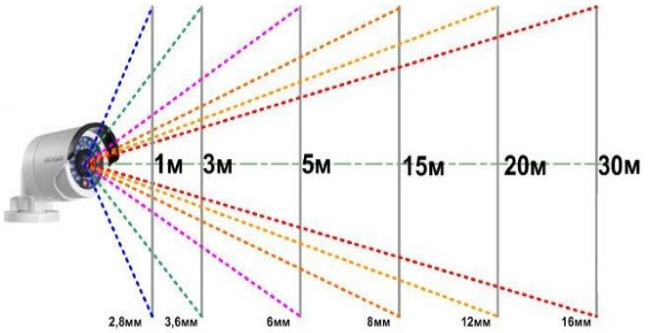

Рис 4. Зависимость угла обзора от фокусного расстояния[13]

Таким образом, выбор камер для проектируемой системы будет зависеть от их места размещения в помещениях. Для офисных помещений будет достаточно камер с фокусным расстоянием от 3,6 мм и углом обзора 72°. В случае размещения камеры на улице фокусное расстояние будет соответственно больше.

Отдельного исследования в рамках разработки и оптимизации алгоритма распознавания потребует размер зоны распознавания для конкретных камер видеонаблюдения.

IV. Концептуальная модель разрабатываемой СКУД

В качестве аппаратно-программного решения планируется разработка автоматизированной СКУД на основе системы видеонаблюдения с встроенной системой распознавания лиц.

Разрабатываемая система как комплексное решение должна выполнять следующие функции:

1) детектирование и распознавание сотрудников и посетителей организации;
2) быстрое выявление несанкционированного доступа в помещениях организации;
3) оповещение о несанкционированном доступе;
4) обеспечение возможности организации пропускного режима на основе биометрии;
5) возможность создания системы допусков разного уровня секретности.

В соответствии с выделенными функциями всю

систему можно разделить на блоки (подсистемы). В будущем это позволит наиболее удобным способом описать работу аппаратно-программного комплекса и применяемые в нем алгоритмы:

1) подсистема видеонаблюдения;
2) подсистема хранения данных;
3) подсистема формирования отчетности;
4) подсистема идентификации.

Диаграмма пакетов для программной части представлена на рис. 5.

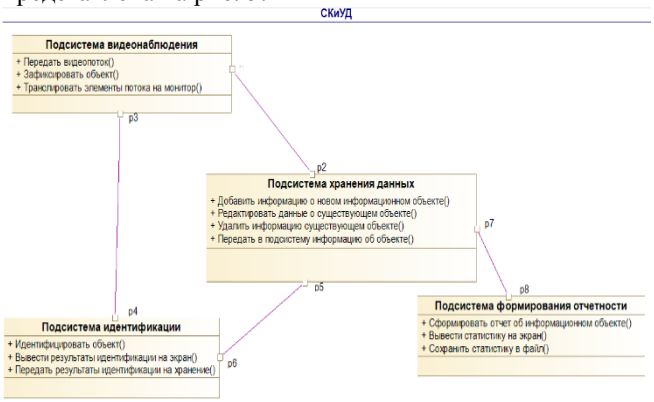

Рис 5. Диаграмма пакетов СКУД

Отдельно в таблице 1 представлена реализация перечисленных подсистем на аппаратном и программном уровне.

Таб. 1. Реализация подсистем на разных уровнях.

Подсистема	**Аппаратный уровень**	**Программный уровень**
Подсистема видеонаблюдения	IP-камеры видеонаблюдения, серверная и сетевая часть для передачи и хранения видеопотока	Клиент-серверное приложение для передачи данных с камер и отображения их в интерфейсе клиента.
Подсистема хранения данных	Сервер с размещенной БД	Клиент-серверное приложение для работы с данными БД
Подсистема формирования отчетности	Сервер с размещенной БД	Клиент-серверное приложение для работы с данными БД
Подсистема идентификации	Сервер для вычислений и микроконтроллеры, датчики движения	Нейронная сеть для детектирования и распознавания, клиент-серверное приложение для отправки и получения результатов идентификации

Для подготовки MVP планируется создание прототипа аппаратно-программного комплекса, состоящего из двух камер, датчиков движения, микроконтроллеров, базы данных и Web-приложения с интерфейсом пользователя.

V. Заключение

Рынок систем безопасности, в том числе и систем контроля и управления доступом, активно развивается в настоящее время. Ежегодный прирост рынка составляет около 5% [16]. При этом, несмотря на существующие готовые решения в сфере СКУД, они обладают рядом описанных ранее проблем, что открывает возможность создания новых продуктов для устранения недостатков существующих автоматизированных систем.

В рамках разработки новой системы контроля и управления доступом является целесообразным выбор подходящих для целей детектирования и распознавания объектов камер на основе их оптических характеристик. Такими характеристиками выступают фокусное расстояние (f') и угол обзора камеры (α). Оптимальными для использования являются цифровые камеры с фокусным расстоянием от 3,6 мм и углом обзора 72°.

Конструктивно разрабатываемая автоматизированная система должна состоять из подсистем видеонаблюдения, хранения данных, формирования отчетности и подсистемы идентификации. Такое разбиение на функциональные блоки поможет на этапе проектирования наиболее точно описать технические и функциональные требования в виде технического задания.

Среди основных функций, которые будет выполнять система, можно выделить детектирование и распознавание сотрудников и посетителей организации, быстрое выявление несанкционированного доступа в помещениях и оповещение о нем, обеспечение возможности организации пропускного режима на основе биометрии и создание системы допусков разного уровня секретности.

Библиография

[1] Шаньгин В. Ф. Комплексная защита информации в корпоративных системах. М. : ФОРУМ-ИНФРА. –2010. –591 с.
[2] ФаткулинА. Н., ОкладниковаЕ. Н., СухаревЕ. Н.Анализ современных систем контроля и управления доступом // Актуальные проблемы авиации и космонавтики. –2011.– С. 263–264.
[3] Волхонский В.В. Системы контроля и управления доступом.СПб: Университет ИТМО. –2015. –105 с.
[4] Рекомендации: выбор и применение систем контроляи управления доступом. М.: ФГУ НИЦ «Охрана» МВД России. –2011. –95 с.
[5] Контрольно-пропускной режим на предприятии // Studbooks.net. –2010(https://studbooks.net/1087938/pravo/obschie_polozheniya_organizatsii_kontrolno_propusknogo_rezhima).
[6] Методика организации контрольно-пропускного режима на предприятии (организации) // официальный сайт города Нижний Тагил. –2010 (https://ntagil.org/bezopas/info.php?SECTION_ID=1216).
[7] Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. М.: Горячая линия–Телеком. –2013. –272 с.
[8] Чепурин И., Птицын Н. От аналога к цифре: обзор решений систем видеонаблюдения // Компоненты и Технологии. –2010. - № 6.–С. 67–68.
[9] Ptz камеры видеонаблюдения: управление, характеристики и особенности // Ваш дом. Техника и ремонт (https://technika-remont.ru/ispolzovanie-ptz-kamer-v-sistemah-videonabludenia/).
[10] Титов. Ф. HD-SDI и EX-SDI — стандарты видеонаблюдения // Интемс (https://securityrussia.com/blog/hd-sdi.html).
[11] Рожков П. Сетевые камеры. 10 причин купить сетевую камеру // T-Comm - Телекоммуникации и Транспорт. – 2009. –С. 47–49.
[12] Функциональная схема видеокамеры//helpiks.org. –2014 (https://helpiks.org/8-3504.html)
[13] Обзор основных характеристик оборудования для систем видеонаблюдения// Редан. Комплексные системы безопасности (https://redan-guard.ru/stati/1147-obzor-harakteristik-oborudovaniya-sistem-videonablyudeniya).
[14] Особенности выбора камер видеонаблюдения для систем цифровой аналитики// Амиком. Системы безопасности. –2019 (https://www.ami-com.ru/articles/aktualnye-standarty-obnaruzheniya-raspoznavaniya-i-identifikatsii-dlya-sistem-videonablyudeniya/).
[15] Шуругин С. В., Енчинов А. А., Грицкевич Е. В. Использование метода статистического моделирования для идентификации объекта по геометрическим параметрам его изображения // Интерэкспо Гео-Сибирь. –2021.– С. 314–320.

[16] На 5% ежегодно будет расти рынок СКУД до 2025 года // Rubеж. – 2021(https://ru-bezh.ru/kompanii-i-ryinki/news/21/02/08/na-5-ezhegodno-budet-rasti-ryinok-skud-do-2025-goda).

Analysis of the approaches to the development control access systems

A. B. Mudrich, K.V.Ezhova

Abstract—The article discusses a conceptual approach to the development of an access control system for company based on the biometrics technologies.
One of the most important tasks for every organization is to maintain a high level of security by using different access control systems on own territory. In the presented work, a special place is given to video monitoring systems with face recognition function. Typically, such systems are a complex of hardware and software elements where intellectual analysis based on computer vision algorithms. There are several strict requirements for the hardware and programming levels of this systems. Cameras must provide a high quality of the video for recognition and detection objects. Software must be enough fast for working as real–time system and the recognition algorithm must have a high accuracy.
The first section of the article discusses the concept of access control systems. The second section contains the basic technical requirements for video monitoring systems with object recognition function. The third section contains the access control system concept and description of it developing during future scientific and engineering work.

***Keywords*—access control system, face recognition, video monitoring system, security system.**

REFERENCES

[1] Shangin V. F. Complex information protection in corporate systems.Moscow : FORUM-INFRA. – 2010. –591 p.
[2] Fatkullin A. N., Okladnikova E. N., Sukharev E. N. Analysis of modern access control systems // Actual problems of aviation and cosmonautics. –2011. –P. 263-264.
[3] Volkhonsky V. V. Access control systems. St. Petersburg: ITMO University. –2015. –105 p.
[4] Recommendations: the choice and application of access control systems. Moscow: Federal State Institution SIC "Protection" of the Ministry of Internal Affairs of Russia. –2011. –95 p.
[5] The checkpoint regime in organization // Studbooks.net. – 2010 (https://studbooks.net/1087938/pravo/obschie_polozheniya_organizatsii_kontrolno_propusknogo_rezhima).
[6] Methodology of the organization of the checkpoint regime in organization // official website of the city of Nizhny Tagil –2010 (https://ntagil.org/bezopas/info.php?SECTION_ID=1216).
[7] Vorona V. A., Tikhonov V. A. Access control systems. Moscow: Hotline–Telecom. –2013. –272 p.
[8] Chepurin I., Ptitsyn N. From analog to digital: a review of video monitoring system solutions // Components and Technologies. –2010. - Vol. 6. –P. 67-68.
[9] PTZ video cameras: management, characteristics and features // Your home. Equipment and repairs (https://technika-remont.ru/ispolzovanie-ptz-kamer-v-sistemah-videonabludenia/).
[10] Titov. F. HD-SDI and EX-SDI — video surveillance standards // Intems (https://securityrussia.com/blog/hd-sdi.html).
[11] Rozhkov P. Network cameras. 10 reasons to buy a network camera // T-Comm - Telecommunications and Transport. –2009. –P. 47-49.
[12] Functional diagram of the video camera // helpiks.org. –2014 (https://helpiks.org/8-3504.html)
[13] Overview of the main characteristics of equipment for video monitoring systems // Redan. Integrated security systems (https://redan-guard.ru/stati/1147-obzor-harakteristik-oborudovaniya-sistem-videonablyudeniya).
[14] Features of the choice of video cameras for digital analytics systems // Amikom. Security Systems 2019 (https://www.ami-com.ru/articles/aktualnye-standarty-obnaruzheniya-raspoznavaniya-i-identifikatsii-dlya-sistem-videonablyudeniya/).
[15] Shurugin S. V., Enchinov A. A., Gritskevich E. V. Using the statistical modeling method to identify an object by geometric parameters of its image // Interexpo Geo-Siberia. – 2021.–P. 314-320.
[16] The ACS market will grow by 5% annually until 2025 // Rubez. – 2021(https://ru-bezh.ru/kompanii-i-ryinki/news/21/02/08/na-5-ezhegodno-budet-rasti-ryinok-skud-do-2025-goda).