

Система контроля и управления доступом

11, ноябрь 2014

Бойко А. А., Мамаев В. Ю.

УДК: 004.93'1

Россия, МГТУ им. Н.Э. Баумана

boiko_andrew@mail.ru

Введение

Использование систем контроля и управления доступом (СКУД) является одним из наиболее эффективных способов обеспечения комплексной безопасности различных объектов. Традиционно в составе СКУД выделяют следующие основные компоненты [1]:

- устройства идентификации (идентификаторы и считыватели);
- устройства контроля и управления доступом (контроллеры);
- устройства центрального управления (компьютеры);
- исполнительные устройства (замки, приводы дверей, шлагбаумов, турникетов).

Основным недостатком традиционных СКУД является потенциальная возможность передачи идентификатора одним пользователем Системы другому. Для предотвращения передачи идентификатора возможна его биометрическая персонализация с использованием одной из биометрических модальностей¹, однозначно идентифицирующих пользователя. Наиболее часто в качестве такой модальности используются отпечатки пальцев и, несколько реже, изображение лица, что связано, прежде всего, с относительной простотой получения данных характеристик. Биометрическая СКУД с использованием отпечатков пальцев в течение пяти лет эксплуатируется в МГТУ им. Н.Э. Баумана (в общежитиях № 10, 11). Биометрическая СКУД характеризуется рядом эксплуатационных характеристик, среди которых важнейшими являются вероятность ложного недопуска (когда система ошибочно отказывает в допуске «своему») и вероятность ложного допуска (когда система ошибочно опознает «чужого» как «своего»). Определению двух указанных характеристик посвящена настоящая статья. Таким образом, *объектом исследования* является биометрическая СКУД общежитий № 10, 11, *предметом исследования* – эксплуатационные характеристики СКУД, а *целью работы* – определение указанных эксплуатационных характеристик.

¹ В соответствии с ГОСТ Р 54411 – 2011, биометрическая модальность (biometric modality) – биометрическая характеристика, применяемая в биометрическом процессе.

Для определения эксплуатационных характеристик были проведены эксплуатационные испытания по методике, составленной в соответствии с ГОСТ Р ИСО/МЭК 19795-1 – 2007. При проведении испытаний был использован метод непосредственных наблюдений. Кроме того, для получения информации об общем количестве проходов и их распределении по временным интервалам осуществлялись SQL-запросы к базе данных СКУД.

Описание биометрической системы, перечень эксплуатационных характеристик и порядок их определения, полученные результаты и их обсуждение представлены в последующих пяти разделах данной работы.

1. Описание биометрической системы

Биометрическая система контроля и управления доступом в общежитиях № 10, 11 МГТУ им. Н.Э. Баумана (Автоматизированная система контроля пропускного режима, АСКПР) введена в эксплуатацию 1 ноября 2009 г. приказом Ректора МГТУ им. Н.Э. Баумана № 31-03/1329 и функционирует в круглосуточном режиме по настоящее время. АСКПР разработана научно-исследовательским и испытательным центром биометрической техники МГТУ им. Н.Э. Баумана совместно с кафедрами БМТ-1 и ИУ-5 МГТУ им. Н.Э. Баумана на основании утвержденного технического задания шифр «Основа-АВОБ» от 7 февраля 2008 г.

По функциональному назначению АСКПР разделена на два *сегмента*:

- сегмент «Объект», размещенный на территории общежитий № 10, 11;
- сегмент опытного стенда, размещенный в ауд. 147 Учебно-лабораторного корпуса.

Сегмент «Объект» включает три компонента:

- бюро пропусков;
- центральный сервер Объекта;
- контрольно-пропускной пункт (КПП)².

Сегмент опытного стенда включает два компонента:

- автоматизированное рабочее место сбора персональных и биометрических данных;
- автоматизированное рабочее место изготовления пропускных документов.

В качестве *идентификатора* [1] используется карта идентификационная бесконтактная индукционная (КИБИ-002 МТ). КИБИ-002 МТ построен на основе БИС КБ5004ХК1 - бесконтактного пассивного ответчика-идентификатора, представляющего собой однократно программируемое ПЗУ, считывание информации из которого и электропитание производятся по встроенному радиоканалу, работающему на частоте 13,56

² В настоящее время в составе сегмента «Объект» функционирует два контрольно-пропускных пункта – КПП 1 и КПП 2.

МГц. В качестве *считывателя* используется считыватель радиочастотных карт с интерфейсом RS485. Для *персонализации идентификатора* (электронного пропускного документа, ЭПД) используется двусторонний полноцветный принтер в сборе с двусторонним ламинационным модулем Fargo HDP5000 DS LAM2, осуществляющий печать по термотрансферной технологии. В качестве биометрической модальности используется шаблон отпечатка пальца, изображение отпечатка пальца регистрируется с помощью *сканера отпечатков пальцев Futronic FS83C*. В качестве *устройства заграждения* используется полуростовой турникет «Ростов-Дон Р2М1/3». Схема АСКПР представлена на рис. 1.

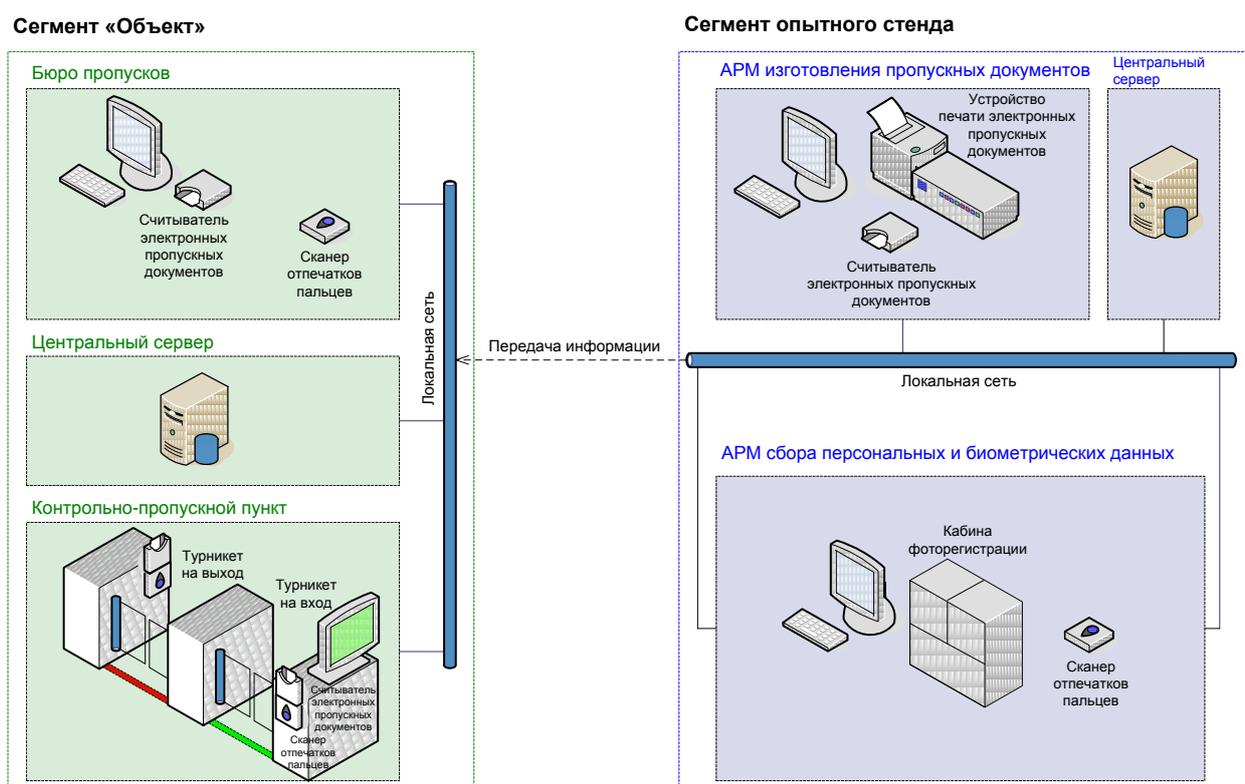


Рис. 1. Схема АСКПР

Вход в общежитие осуществляется по идентификатору и отпечатку пальца, выход – только по идентификатору. При этом специальным программным обеспечением осуществляется контроль, исключающий возможность двойного прохода на вход или выход. Эксплуатационные характеристики определялись при входе в общежитие.

2. Эксплуатационные характеристики

В автоматизированной системе контроля пропускного режима (АСКПР) общежитий № 10, 11 работа биометрической системы осуществляется в режиме верификации.

Согласно ГОСТ Р ИСО/МЭК 19795-1 [3], *верификацией* называют процесс, при котором происходит сравнение представленного пользователем образца с шаблоном, зарегистрированным в базе данных; при этом признаки передаваемого пользователем образца сравниваются с зарегистрированным шаблоном и по результатам сравнения возвращается положительное или отрицательное решение о запрошенной идентичности.

Биометрическая система, функционирующая в режиме верификации, характеризуется следующими эксплуатационными характеристиками:

- вероятность отказа регистрации, ВОР (failure-to-enroll rate; FTE);
- вероятность отказа сбора данных, ВОСД (failure-to-acquire rate; FTA);
- вероятность ложного несовпадения, ВЛНС (false non-match rate; FNMR);
- вероятность ложного совпадения, ВЛС (false match rate; FMR);
- вероятность ложного недопуска, ВЛНД (false reject rate; FRR);
- вероятность ложного допуска, ВЛД (false accept rate; FAR).

В соответствии с ГОСТ Р ИСО/МЭК 19795-1 [3], *вероятность отказа регистрации* – доля выборки, для которой система не может завершить процесс регистрации.

Вероятность отказа сбора данных – доля попыток верификации, для которых система не может получить или отобразить изображение или сигнал удовлетворительного качества.

Вероятность ложного несовпадения – доля образцов, полученных в результате попыток подлинного лица, которые ошибочно признаны не совпадающими с шаблоном той же биометрической характеристики данного пользователя, представившего образец.

Вероятность ложного совпадения – доля образцов, полученных в результате пассивных попыток «самозванца», которые ошибочно признаны совпадающими с шаблоном другого пользователя.

Вероятность ложного недопуска – доля транзакций верификации подлинного лица, которые будут ошибочно отвергнуты.

Вероятность ложного допуска – доля транзакций верификации «самозванца», которые будут ошибочно приняты

ВЛНД определяют как весовую долю записанных транзакций подлинного лица, которые были ошибочно отвергнуты. Сюда же входят транзакции, отвергнутые из-за отказа сбора данных и ошибок соответствия. ВЛНД равна (1):

$$\text{ВЛНД} = \text{ВОСД} + \text{ВЛНС} \cdot (1 - \text{ВОСД}). \quad (1)$$

ВЛД определяют как весовую долю записанных пассивных транзакций «самозванца», которые были ошибочно приняты (2):

$$\text{ВЛД} = \text{ВЛС} \cdot (1 - \text{ВОСД}). \quad (2)$$

Поскольку вероятность отказа сбора данных, а также вероятность ложного совпадения и вероятность ложного несовпадения в существующих условиях эксплуатации АСКПР определить невозможно, в качестве эксплуатационных характеристик АСКПР в настоящей работе рассматриваются только вероятность ложного недопуска и вероятность ложного допуска.

3. Методика испытаний

Для определения вероятности ложного недопуска было предложено наблюдение за процессом функционирования АСКПР в течение суток, в предположении, что за это время все сотрудники и проживающие в общежитиях хотя бы один раз пересекут охраняемый периметр. В таком случае ВЛНД будет определена как доля проходов, при которых открытие турникета вынужденно осуществлялось в ручном режиме, от общего количества проходов внутрь охраняемого периметра³.

С учетом того, что общее количество сотрудников и проживающих в общежитии составляет около 3 000 человек, с доверительной вероятностью 95 % ошибка определения ВЛНД по «правилу трех» [3] (3) будет равна (или меньше)

$$p_1 \approx 3/N_1 = 3/3000 = 0,001 (0,1 \%). \quad (3)$$

Для определения ВЛД на первом этапе предполагалось смоделировать 300 попыток прохода «самозванцев». В этом случае с доверительной вероятностью 95 % ошибка определения ВЛД по «правилу трех» [3] (4) будет равна (или меньше)

$$p_2 \approx 3/N_2 = 3/300 = 0,01 (1 \%). \quad (4)$$

4. Результаты испытаний

Испытание для определения вероятности ложного недопуска проводилось в течение суток с 8.00 22.11.2013 до 8.00 23.11.2013. За этот период не зафиксированы ошибочно отвергнутые транзакции подлинного лица, следовательно

$$\text{ВЛНД} = 0/N \cdot 100 \% = 0 \%,$$

где N – число проходов за данный период.

Общее число проходов составило 2 862. Совокупный объем проходов и распределение этого объема по часам представлено в табл. 1, а также на рис. 1 и рис. 2.

³ Открытие турникета в ручном режиме может быть вызвано и другими причинами, отличными от ошибки ложного недопуска, например, такая ситуация имеет место при проходе по разовому или временному пропуску. Поэтому для определения ВЛНД необходимо учитывать только случаи использования постоянного пропуска и связанный с ними результат верификации по изображению отпечатка пальца.

Таблица 1. Совокупный объем проходов через турникеты КПП 1 и КПП 2 АСКПР 22.11.2013

Интервал времени	Турникет КПП 1	Турникет КПП 2
8.00 – 9.00	4	5
9.00 – 10.00	20	34
10.00 – 11.00	23	49
11.00 – 12.00	34	70
12.00 – 13.00	52	88
13.00 – 14.00	63	131
14.00 – 15.00	67	133
15.00 – 16.00	86	189
16.00 – 17.00	93	168
17.00 – 18.00	91	186
18.00 – 19.00	86	137
19.00 – 20.00	98	157
20.00 – 21.00	49	99
21.00 – 22.00	64	112
22.00 – 23.00	53	108
23.00 – 24.00	37	72
0.00 – 1.00	40	63
1.00 – 2.00	20	13
2.00 – 3.00	19	7
3.00 – 4.00	17	1
4.00 – 5.00	9	0
5.00 – 6.00	2	0
6.00 – 7.00	3	5
7.00 – 8.00	1	4

Примечание – Турникет КПП 1 расположен ближе к бюро пропусков, турникет КПП 2 – соответственно, дальше от бюро пропусков. Учитывались только проходы с использованием ЭПД, поэтому для турникета КПП 2 их количество больше. Через турникет КПП 1 осуществляются проходы по временным бумажным пропускам в ручном режиме по нажатию контролером на кнопку, поэтому число автоматических проходов, зарегистрированных системой для турникета КПП 1, меньше.

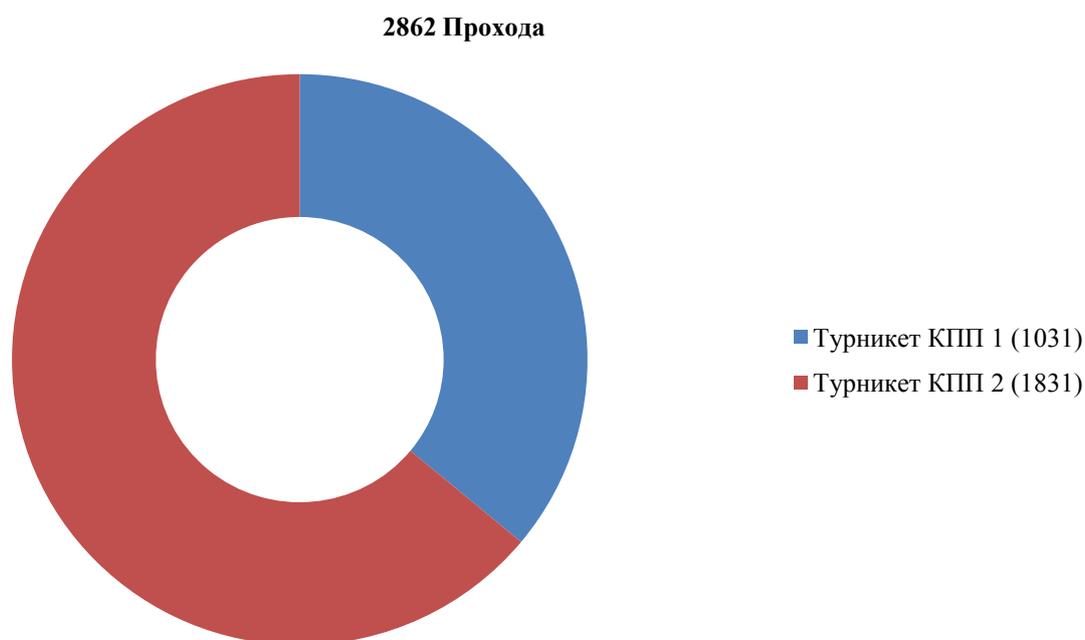


Рис. 2. Совокупное распределение числа проходов по турникетам КПП 1 и КПП 2

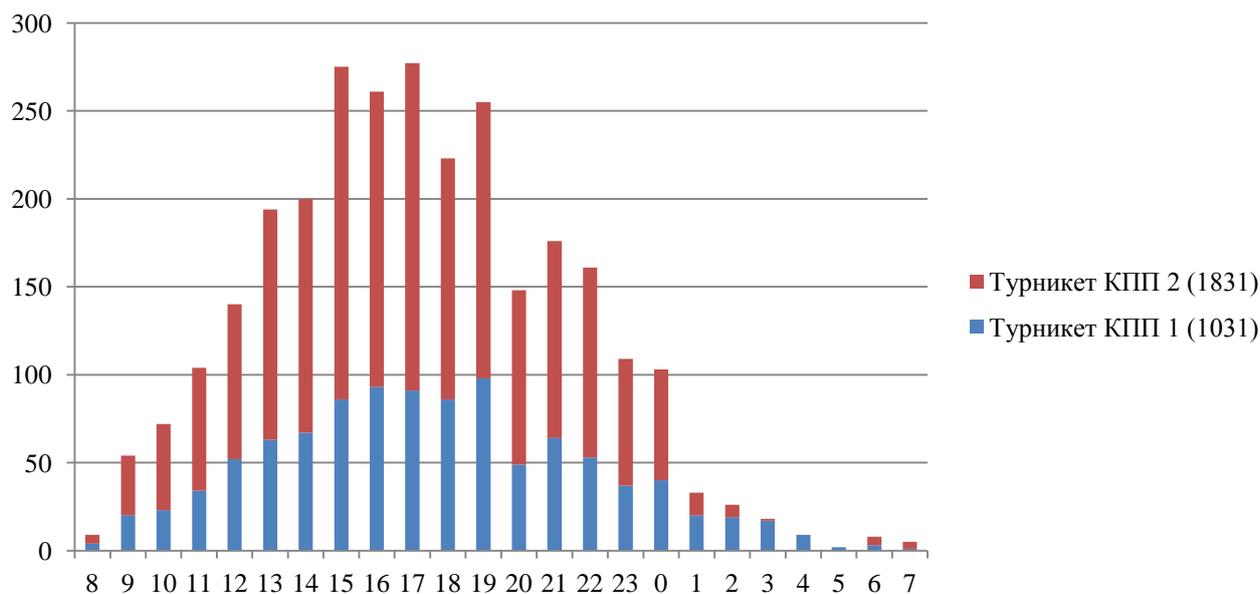


Рис. 3. Распределение числа проходов по турникетам КПП 1 и КПП 2 по интервалам времени

Испытания для определения вероятности ложного допуска проводились дважды. Первое испытание проводилось 28.11.2013 в интервале времени с 14.30 до 15.50. За это время было осуществлено 135 попыток проходов различных лиц по пропуску другого пользователя (транзакций «самозванца»). Количество успешно прошедших лиц (транзакций «самозванца», которые были ошибочно приняты) составило 13. Таким образом, вероятность ложного допуска в первом испытании составляет:

$$ВД_1 = 13/135 \cdot 100 \% = 9,6 \%$$

Второе испытание проводилось 09.01.2014 в интервале времени с 11.40 до 13.50. За это время было осуществлено 300 проходов различных лиц по пропуску другого пользователя (транзакций «самозванца»). Количество успешно прошедших лиц (транзакций «самозванца», которые были ошибочно приняты) составило 13. Вероятность ложного допуска во втором испытании составляет:

$$ВД_2 = 13/300 \cdot 100 \% = 4,3 \%$$

Результаты определения вероятности ложного допуска проведенных испытаний обобщены в табл. 2.

Таблица 2. Результаты определения вероятности ложного допуска

Дата испытания	Интервал времени	Количество проходов, шт.	Количество успешных проходов по пропуску другого пользователя, шт.	ВД, %
2013.11.28	14.30 – 15.50	135	13	9,6
2014.01.09	11.40 – 13.50	300	13	4,3
Среднее значение				7,0

Среднее значение вероятности ложного допуска по итогам проведенных испытаний составило 7,0 %.

5. Анализ результатов

По итогам проведенных эксплуатационных испытаний получены следующие значения:

- вероятность ложного недопуска (ВЛНД) – 0 %;
- вероятность ложного допуска (ВЛД) – 7,0 %.

При создании автоматизированной системы контроля пропускного режима настройка системы была выполнена таким образом, чтобы минимизировать вероятность ложного недопуска. На вероятность ложного недопуска влияют климатические факторы – температура и влажность пальцев, которые влияют на качество получаемого шаблона отпечатка пальца. Было принято решение об уменьшении вероятности ложного недопуска путем уменьшения порога принятия решения о положительном результате верификации. При этом фактическая вероятность ложного допуска весьма мала из-за отсутствия обмена пропусками между студентами и визуального контроля лица сотрудником охраны при проходе.

ВЛНД в зависимости от ВЛД принято изображать с помощью кривой компромиссного определения ошибки или кривой рабочей характеристики. В соответствии с ГОСТ Р ИСО/МЭК 19795-1 [3], *кривая компромиссного определения ошибки, кривая КОО* (detection error trade-off curve; DET curve) – модифицированная кривая рабочей характеристики, по осям которой отложены вероятности ошибки (ложноположительная – по оси X и ложноотрицательная – по оси Y). Пример кривой КОО приведен на рис. 4.

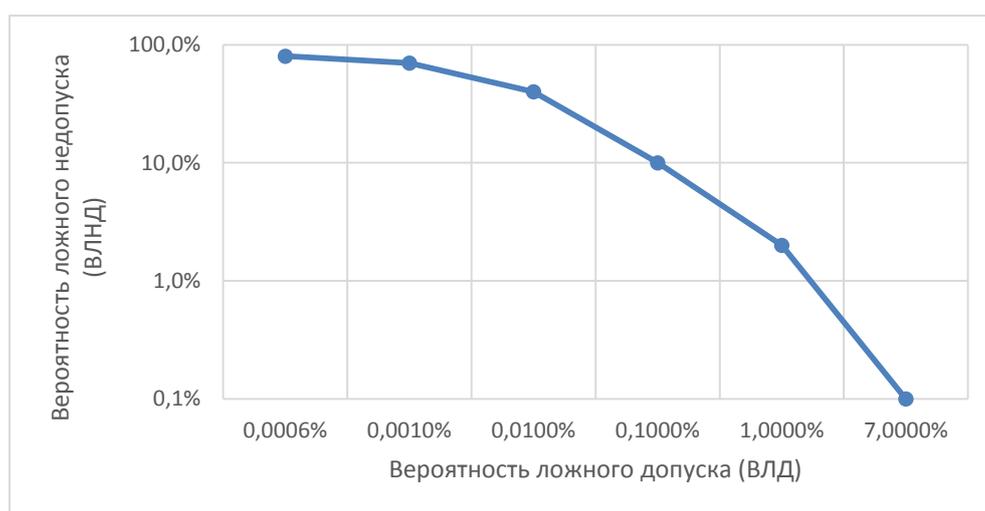


Рис. 4. Пример кривой КОО

Анализ кривой, изображенной на рис. 4, позволяет сделать следующий вывод: уменьшение вероятности ложного допуска возможно при увеличении вероятности ложно-

го недопуска, что фактически соответствует смещению рабочей точки по кривой КОО влево. При этом при значении ВЛНД 10 % ВЛД составляет 0,1 %, что является стандартным значением для систем данного класса. Однако при этом из-за увеличения количества транзакций ⁴ неизбежно происходит уменьшение пропускной способности, что для рассматриваемой биометрической системы является критичным из-за достаточно высокой нагрузки на КПП в отдельные часы (см. интервал времени с 19.00 до 20.00 в табл. 1). Таким образом, данный вариант снижения вероятности ложного допуска является неприемлемым. Необходимо решение, которое при фиксированном значении вероятности ложного недопуска позволит уменьшить вероятность ложного допуска. Одним из возможных вариантов является мультимодальная биометрическая система, которая помимо шаблона отпечатка пальца использует одну или несколько дополнительных биометрических модальностей, например, 2D- или 3D-изображение лица. Реализация мультимодальной биометрической системы позволит устранить необходимость визуального сопоставления сотрудником охраны лица человека с изображением из базы данных.

Методы идентификации по изображению лица традиционно разделяют на две группы:

- методы, основанные на геометрических признаках;
- методы, основанные на признаках внешнего вида.

При создании автоматизированной системы паспортного контроля в международном аэропорту «Шереметьево» Научно-исследовательским и испытательным центром биометрической техники МГТУ им. Н.Э. Баумана был реализован алгоритм идентификации по лицу с помощью метода, основанного на геометрических признаках, с вероятностью ложной идентификации на закрытом множестве, не превышающей 4 %.

В настоящее время ведутся работы с перспективой интеграции в состав АСКПП данного алгоритма, а также системы некооперативного распознавания лиц VOCORD FaceControl 2D и 3D.

Заключение

Проведенные эксплуатационные испытания показали, что АСКПП общежитий № 10, 11 характеризуется низкой вероятностью ложного недопуска при недостаточно низкой вероятности ложного допуска в выбранной точке кривой компромиссного определения ошибки. Уменьшение ВЛД возможно одним из следующих способов:

- увеличение порога принятия решения о положительном результате верификации, что повысит вероятность ложного недопуска и, следовательно, приведет к уменьшению пропускной способности Системы;
- использование дополнительных биометрических модальностей и создание мультимодальной биометрической СКУД – в случае, если значения вероятностей ложного

⁴ В соответствии с ГОСТ Р ИСО/МЭК 19795-1 – 2007, транзакция (transaction) – последовательность попыток со стороны пользователя для регистрации, верификации или идентификации.

недопуска и ложного допуска в рабочей точке на кривой КОО не будут удовлетворять заданным вероятностям.

Последний из предложенных вариантов представляется наиболее предпочтительным, и в настоящее время ведутся работы по его реализации.

Список литературы

1. ГОСТ Р 54411 – 2011. Информационные технологии. Биометрия. Мультимодальные и другие мультибиометрические технологии. Введ. 2011-09-21. М.: Стандартиформ, 2014. 32 с.
2. Котов Н.Н., Савчук Л.И., Тюрин Е.П., Синилов В.Г. Выбор и применение систем контроля и управления доступом: Рекомендации. – М.: НИЦ «Охрана», 1999. 63 с.
3. ГОСТ Р ИСО/МЭК 19795-1 – 2007. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура. Введ. 2008-12-25. М.: Стандартиформ, 2009. 57 с.