ВНЕДРЕНИЕ БИОМЕТРИИ В СИСТЕМЫ КОНТРОЛЯ ДОСТУПА НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

IMPLEMENTATION OF BIOMETRICS IN ACCESS CONTROL SYSTEMS AT CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

УДК 004.056.52

DOI: 10.24411/2658-4964-2021-10347

Зудинов Антон Сергеевич, студент 2 курс, магистр, кафедра КБ-1 «Защита информации», Институт комплексной безопасности и специального приборостроения, РТУ МИРЭА, Россия, г. Москва

Zudinov Anton Sergeevich, student 2 course, Master, Department KB-1, "Information Security", Institute of Integrated Security and Special Instrumentation, RTU MIREA, Russia, Moscow

Аннотация: Статья посвящена внедрению биометрии в системы контроля доступом на объектах критической информационной инфраструктуры, ее преимущества и недостатки. В статье рассматриваются такие аспекты как виды биологических идентификаторов таких как отпечатки пальцев, сетчатку глаза, рисунок вен и распознавание по лицу. Описывается преимущество внедрения многофакторной аутентификации. Так же рассматриваться такие показатели биометрических систем как FAR и FRR являющиеся основными для оценки и сравнения идентификаторов.

Annotation: The article is devoted to the introduction of biometrics into access control systems at critical information infrastructure facilities, its advantages and disadvantages. The article discusses aspects such as types of biological identifiers such as fingerprints,

retina, vein pattern and face recognition. Describes the benefits of implementing multi-factor authentication. Such indicators of biometric systems as FAR and FRR, which are the main ones for evaluating and comparing identifiers.

Ключевые слова: информационная безопасность, биометрия, контроль доступа, СКУД, КИИ, идентификация

Keywords: information security, biometrics, access control, Access Control System, critical information infrastructure, identification

Введение

В сфере защиты информации термин «контроль доступа» является набором средств от проникновения в охраняемую зону, санкционированный допуск на защищаемую территорию возможен только для авторизованных пользователей, получивших на это разрешение. Простейший физический контроль возможно реализовать путем найма персонала (охранник или консьерж), механическими средствами, такими как ключи и замки на двери, или через технические средства. В связи с ростом технологий биометрические системы контроля доступа становятся все более доступным и популярным решением. Биометрия считается более безопасной по отношению к обычным СКУД, так как сравнивает уникальные для каждого человека показатели (отпечатки пальцев, радужная оболочка глаза, геометрия лица, голос)

Сравнение видов идентификаторов СКУД

Рассматривая идентификаторы использующие физические носители (магнитные, механические, электронные контактные и радиочастотные) можно заметить существенный недостаток, заключающийся в возможности хищения или подделки идентификатора. Эта возможность сильно снижает общий уровень безопасности на любом защищаемом объекте. Что бы максимально снизить риски связи с данной проблемой можно использовать биометрические считыватель, которые предназначены для идентификации пользователей на основе уникальных физиологических особенностей. Из этого следует что для объектов, где они

установлены значительно снизился риск несанкционированного доступа эти объекты.

Есть много типов физиологических идентификаторов, основные из них:

- Отпечаток пальца
- Радужная оболочка глаза
- Сетчатка глаза
- Рисунок вен
- Распознавание лица 3D

Биометрические системы могут состоять как из аппаратного, так и из программного обеспечения. Биометрический прибор идентификации собирает, считывает и сравнивает биометрические данные. Биометрические данные-это комплекс данных, из которых нужно извлечь уникальные данные для пользователя. Внедренное программное обеспечение внутри биометрической системы включает в себя “биометрический двигатель”, который обрабатывает собранные биометрические данные. Программа обычно работает в комплексе с оборудованием для управления процессом сбора биометрических данных, оборудованием извлечения данных и проведения сравнения, включая сопоставление данных [1].

В биометрических СКУД существуют недостатки свойственные только данным типам систем. Биосистемы не предусматривают выдачу временных пропусков [5]. На данный момент в отличие от физических идентификаторов есть вероятность не распознать биометрические параметры, это связано в первую очередь с наличием вероятностных и динамических характеристик, например, запотевание и высыхание ладоней. Нестабильность падает в зависимости от вида считывателя. Главными, для оценки любой биометрической системы, являются два параметра:

FAR (False Acceptance Rate) - коэффициент ложного пропуска, т.е. процент возникновения ситуаций, когда система разрешает доступ пользователю, незарегистрированному в системе.

FRR (False Rejection Rate) - коэффициент ложного отказа, т.е. отказ в доступе настоящему пользователю системы.

Обе характеристики получают расчетным путем на основе методов математической статистики. Чем ниже эти показатели, тем точнее распознавание объекта.

Для самых популярных на сегодняшний день методов биометрической идентификации средние значения FAR и FRR выглядят следующим образом[2]:

Биометрическая СКУД использует:	**FAR**	**FRR**
Отпечаток пальца	0,001%	0,6%
Распознавание лица 3D	0,0005%	0,1%
Радужная оболочка глаза	0,00001%	0,016%
Сетчатка глаза	0,0001%	0,4%
Рисунок вен	0,0008%	0,01%

Таблица 1. Средние значения FAR и FRR.

Для наглядности представлю эти данные в виде диаграммы:

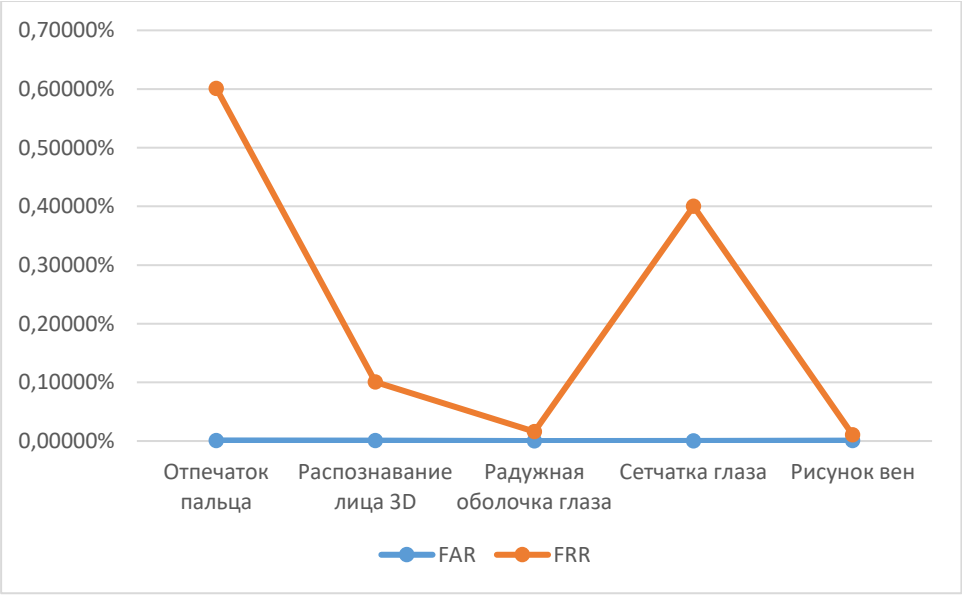

Диаграмма 1. Средние значения FAR и FRR.

С другой стороны, биометрия может уменьшить вероятность несанкционированного доступа традиционных систем доступа. Отсутствие

возможности передачи идентификаторов другому пользователю позволяет эффективно взаимодействовать СКУД с системой учета рабочего времени.

Так как биометрический идентификатор нельзя забыть или потерять – существенно возрастает надежность пропускной системы, особенно актуально для крупных объектов с постоянной текучкой постоянных пользователей, например, студенческие общежития.

На сегодняшний день на рынке доминируют технологии распознавания лица, отпечатков пальцев, радужной оболочки глаза.

По сфере применения лидируют гос. Проекты и банковская сфера.

По географическому распределению лидирует на рынке биометрических систем Северная Америка (более 40% мирового рынка в 2015 году). Активный рост прогнозируется в Китае и Японии.

В частном случае внедрение биометрической идентификации в СКУД позволяет получить ряд преимуществ, а именно:

- Отсутствие смарт карт или токенов позволяет защититься от их потери или хищения, параллельная интеграция на рабочие места позволит повысить общую защищенность ИС;
- Уникальность биометрических параметров не позволит злоумышленнику получить доступ на объект;
- Внедрение позволит сэкономить на пропусках, а также на оборудовании для их программирования;

Применение биометрических устройств является оправданным не только при организации СКУД, но и при создании систем учета рабочего времени (СУРВ), так как необходимость предъявления уникального признака полностью исключает возможность подлога при проходе, что обеспечивает корректный учет отработанного сотрудником времени [3].

Рекомендации по внедрению в системы КИИ

Биометрия может быть хорошей дополнительной процедурой СКУД, работающей в автоматизированных системах на объектах критической информационной

инфраструктуры, повышая качественно повышая уровень безопасности как отдельная ступень идентификации или как один из этапов аутентификации.

Стоит отметить разницу между биометрической идентификацией и верификацией, а именно верификация совершает малое количество сопоставлений, как правило один к одному, с другой стороны особенностью биометрической идентификации является наличие крупной биометрической базы данных при которой образцы будут сравнивается с каждой записью в базе данных, что требует высокой производительности системы в обратном случае можно использовать более дешёвую ЭВМ. Из этого следует что при использовании биометрии в качестве идентификатора используется больше ресурсов ЭВМ. Соответственно лучшем решением будет сделать биометрию не единственной ступенью защиты, а частью процедуры верификацией на объектах КИИ. Еще одним немало важным фактором применению биометрии как дополнительной функции системы защиты является появление многофакторной аутентификации, которая сама по себе является хорошим решением для увеличения защищенности любого объекта, в том числе и объекта КИИ.

Пример типовой схемы интеграции биометрических блоков доступа в СКУД на объектах КИИ [8]:

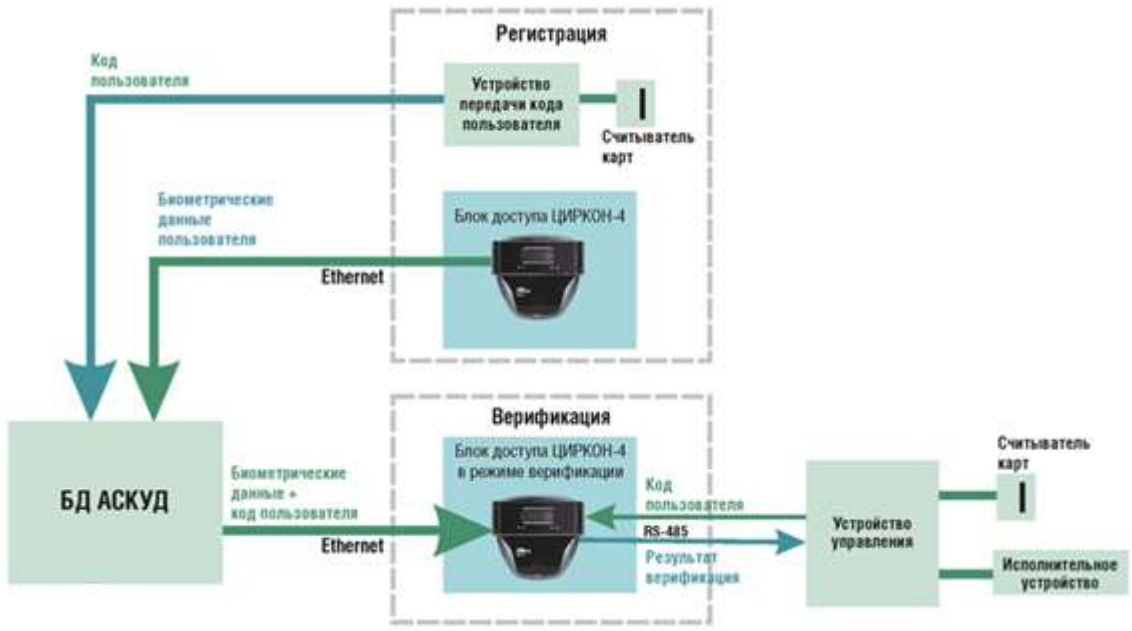

Рисунок 1. Типовая схема интеграции блоков доступа.

Вывод

Технологии, основанные на биометрической идентификации с каждым годом, прилучают все более обширное распространение и популярность как со стороны сотрудников информационной безопасности, так и со стороны пользователей, активно взаимодействующих с ними. Хорошим примером может стать повсеместное внедрение данной технологии в портативные персональные устройства, в частности в смартфоны. Использование данной технологии на объектах КИИ в первую очередь приведёт к повышению общей надежности систем защиты.

Внедрение биометрии на объекты кии уже показала себя с положительной стороны. На данный момент технологией уже пользуются многие банки. Так же вводиться проект под названием Единая биометрическая система направленный на общую идентификацию граждан, пользующихся банковскими услугами по биометрической информации.

Тем не менее основная задача производителей средств защиты и разработчиков СКУД с использованием биометрической идентификации это правильная интеграция средств защиты.

Литература

1. Анализ механизмов защиты информации с использованием биометрических данных [электронный ресурс] URL: https://www.elibrary.ru/item.asp?id=42838168& (дата обращения: 07.04.2021).
2. Биометрическая идентификация [электронный ресурс] URL: http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html (дата обращения: 11.04.2021).
3. Биометрия от «А» до «Я» полное руководство биометрической идентификации и аутентификации [электронный ресурс] URL: https://securityrussia.com/blog/biometriya.html (дата обращения: 11.04.2021).
4. Обзор международного рынка биометрических технологий и их применение в финансовом секторе [электронный ресурс] URL:

https://www.cbr.ru/Content/Document/File/36012/rev_bio.pdf (дата обращения: 11.04.2021).

5. Эффективность биометрических систем контроля и управления доступом при реализации таможенного контроля [электронный ресурс] URL: https://novainfo.ru/article/4909 (дата обращения: 15.04.2021).
6. Бойко А.А. Милевская Ю.С. Вестник Московского университета МВД России 2017г
7. Арутненов В. В. Сравнительный анализ биометрических систем защиты информации. - (Организация информационной работы). 2010, №4.
8. Типовая схема интеграции блоков доступа ПАПИЛОН ЦИРКОН-4 в действующую АСКУД [электронный ресурс] URL: http://www.papillon.ru/rus/50 (дата обращения: 10.05.2021).

Literature

1. Analysis of information protection mechanisms using biometric data [electronic resource] URL: https://www.elibrary.ru/item.asp?id=42838168& (date of access: 07.04.2021).
2. Biometric identification [electronic resource] URL: http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html (date of access: 11.04.2021).
3. Biometrics from "A" to "Z" a complete guide to biometric identification and authentication [electronic resource] URL: https://securityrussia.com/blog/biometriya.html (date of access: 11.04.2021).
4. Overview of the international market of biometric technologies and their application in the financial sector [electronic resource] URL: https://www.cbr.ru/Content/Document/File/36012/rev_bio.pdf (date of access: 11.04.2021).
5. The effectiveness of biometric control and access control systems in the implementation of customs control [electronic resource] URL: https://novainfo.ru/article/4909 (date of access: 15.04.2021).

6. Boyko A.A. Milevskaya Yu.S. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia 2017
7. Arutnenov V. V. Comparative analysis of biometric information security systems. - (Organization of information work). 2010, no. 4.
8. Typical scheme of the PAPILLON ZIRCON-4 access unit in the current ASCUD [electronic resource] URL: http://www.papillon.ru/rus/50 (date of access: 10.05.2021).