# СИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ С БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИЕЙ

# نظام التحكم في الوصول مع المصادقة البيومترية


**Романов Дмитрий Алексеевич**
*Учащийся УО "Национальный детский технопарк"*



**Научный руководитель**
**Бойправ Ольга Владимировна**
*к.т.н., доцент Исполняющий обязанности заведующего кафедры защиты информации БГУИР*

**الشرف العلمي**
**د. أولجا فلاديميروفنا بوبيراف**
أستاذ مشارك القائم بأعمال رئيس قسم أمن المعلومات بجامعة بيلاروسيا الحكومية للاتصالات والمعلوماتية



**Аннотация:** *В работе представлены результаты исследования современных систем управления доступом, а также результаты разработки усовершенствованной системы управления доступом с использованием биометрической аутентификации. В этой системе внедрена нейросеть на базе YOLO для антиспуффинг-защиты, реализованы защита баз данных с использованием шифрования RSA и AES, а также логирование через Elasticsearch. Разработанная система отличается устойчивостью к атакам, высокой скоростью работы и низкими временными затратами, необходимыми для ее развертывания.*



**Ключевые слова**: *Нейросеть, Машинное обучение, Безопасность.*



**ديمتري ألكسيفيتش رومانوف**
طالب في المؤسسة التعليمية "تكنوبارك الوطنية للأطفال"



**الخلاصة :** تقدم هذه الورقة نتائج دراسة أنظمة التحكم في الوصول الحديثة، بالإضافة إلى نتائج تطوير نظام محسن للتحكم في الوصول باستخدام المصادقة البيومترية. يتمتع هذا النظام بشبكة عصبية تعتمد على YOLO للحماية من التزييف وحماية قاعدة البيانات باستخدام تشفير RSA وAES والتسجيل عبر البحث المرن. يتميز النظام المتطور بمقاومته للهجمات وسرعة التشغيل العالية وتكاليف الوقت المنخفضة اللازمة لنشره.



**الكلمات المفتاحية :** الشبكات العصبية، التعلم الآلي، الامن والحماية.


## Введение

С ростом объема обрабатываемых данных и числа угроз в области информационной безопасности системы управления доступом становятся неотъемлемым инструментом защиты. В связи с этим актуальными являются исследования и разработки, направленные на усовершенствование этих систем. Одним из путей усовершенствования систем управления доступом является реализация в рамках них биометрической аутентификации.

## Результаты и обсуждение

Разработанная система управления доступом с биометрической аутентификацией представляет собой интеграцию современных технологий для обеспечения высокого уровня безопасности. Основной акцент сделан на использовании нейросети на базе YOLO для антиспуффинг-защиты, что позволяет эффективно предотвращать атаки с использованием поддельных изображений и видео.

Нейросеть была обучена на реальном датасете, подготовленном с использованием OpenCV. Это обеспечивает высокую точность распознавания лиц и определение подделок в реальных условиях. Обучение проводилось с учетом различных условий освещения, углов обзора и качества изображений, что повысило устойчивость модели к изменениям в окружающей среде [1].

Для защиты данных в системе используются алгоритмы шифрования RSA и AES. RSA обеспечивает безопасную передачу ключей, в то время как AES применяется для шифрования самих данных. Кроме того, реализованы механизмы проверки сложности паролей, что дополнительно защищает учетные записи пользователей от атак методом подбора [2].

Логирование событий реализовано с помощью Elasticsearch, что обеспечивает эффективный мониторинг активности пользователей. Система позволяет быстро анализировать журналы и выявлять подозрительные действия, что способствует повышению общей безопасности системы. Использование Elasticsearch также обеспечивает масштабируемость и высокую скорость обработки запросов.

Система была протестирована на устойчивость к различным типам атак, включая [1-2]:

1. **Подбор паролей**: Реализованная многофакторная аутентификация значительно затрудняет этот тип атаки.
2. **SQL-инъекции**: Применение параметризованных запросов и регулярных проверок кода позволило минимизировать риски.
3. **Атаки спуффинга**: Использование нейросети на базе YOLO для антиспуффинг-защиты продемонстрировало высокую эффективность в идентификации подделок.

По сравнению с существующими решениями, такими как Microsoft Azure Active Directory и Okta Identity Cloud, разработанная система предлагает аналогичный уровень безопасности, но с меньшими затратами на установку и эксплуатацию. Это делает её особенно привлекательной для малых и средних предприятий, которым необходимы надежные решения для управления доступом без значительных финансовых вложений.

## Заключение

Разработанная система управления доступом с биометрической аутентификацией соответствует современным требованиям безопасности и экономической целесообразности. Интеграция нейросетей для антиспуффинг-защиты, применение современных алгоритмов шифрования и эффективное логирование событий делают её надежным инструментом для защиты данных. Данная система существенно повышает уровень безопасности организаций различного размера, обеспечивая защиту от множества потенциальных угроз. Она сочетает биометрическую аутентификацию, нейросети и механизмы шифрования, обеспечивая высокую скорость работы, устойчивость к атакам и низкие затраты на развертывание, что делает её идеальным решением для организаций с ограниченными бюджетами.

## المقدمة

مع نمو حجم البيانات المعالجة وعدد التهديدات في مجال أمن المعلومات، أصبحت أنظمة التحكم في الوصول أداة أمنية متكاملة. وفي هذا الصدد، يعد البحث والتطوير الهادف إلى تحسين هذه الأنظمة أمراً ذا أهمية.

إحدى الطرق لتحسين أنظمة التحكم في الوصول هي تنفيذ المصادقة البيومترية داخلها.

## النتائج والمناقشة

يعد نظام التحكم في الوصول المتطور مع المصادقة البيومترية عبارة عن دمج للتقنيات الحديثة لضمان مستوى عالٍ من الأمان. يركز البحث بشكل أساسي على استخدام الشبكة العصبية القائمة على YOLO للحماية من التزييف، مما يسمح بالوقاية الفعالة من الهجمات باستخدام الصور ومقاطع الفيديو المزيفة.

تم تدريب الشبكة العصبية على مجموعة بيانات حقيقية تم إعدادها باستخدام OpenCV. ويضمن هذا دقة عالية في التعرف على الوجوه واكتشاف المنتجات المزيفة في الظروف الحقيقية. تم إجراء التدريب في ظل ظروف إضاءة وزوايا رؤية وجودة صورة مختلفة، مما زاد من قوة النموذج في مواجهة التغيرات في البيئة [1].

لحماية البيانات، يستخدم النظام خوارزميات التشفير RSA و AES. يوفر RSA نقلًا آمنًا للمفاتيح، بينما يتم استخدام AES لتشفير البيانات نفسها. بالإضافة إلى ذلك، تم تنفيذ آليات للتحقق من تعقيد كلمات المرور، مما يحمي حسابات المستخدمين بشكل أكبر من هجمات القوة الغاشمة [2].

يتم تنفيذ تسجيل الأحداث باستخدام البحث المرن، الذي يوفر مراقبة فعالة لنشاط المستخدم. يتيح لك النظام تحليل السجلات بسرعة وتحديد الأنشطة المشبوهة، مما يساعد على تحسين الأمان العام للنظام. كما يوفر استخدام البحث المرن أيضًا إمكانية التوسع وسرعة عالية في معالجة الاستعلامات.

تم اختبار النظام لمقاومة أنواع مختلفة من الهجمات، بما في ذلك [1-2]:

1. **تخمين كلمة المرور:** إن تطبيق المصادقة متعددة العوامل يجعل هذا النوع من الهجوم أكثر صعوبة.
2. **حقن SQL:** ساعد استخدام الاستعلامات المعلمية والتحقق المنتظم من التعليمات البرمجية في تقليل المخاطر.
3. **هجمات التزييف**: أثبت استخدام الشبكة العصبية القائمة على YOLO للحماية من التزييف كفاءة عالية في تحديد المنتجات المزيفة.

وبالمقارنة بالحلول الموجودة مثل مايكروسوفت أزور الدليل النشط وسحابة الهوية أوكتا ، يوفر النظام المتطور مستوى مماثلاً من الأمان، ولكن بتكاليف تثبيت وتشغيل أقل. وهذا يجعلها جذابة بشكل خاص للشركات الصغيرة والمتوسطة الحجم التي تحتاج إلى حلول موثوقة لإدارة الوصول دون استثمار مالي كبير.

## الخاتمة

يلبي نظام التحكم في الوصول المتطور مع المصادقة البيومترية متطلبات الأمن الحديثة والجدوى الاقتصادية. إن دمج الشبكات العصبية للحماية من التزييف واستخدام خوارزميات التشفير الحديثة وتسجيل الأحداث الفعال يجعلها أداة موثوقة لحماية البيانات. يعمل هذا النظام على زيادة مستوى الأمان بشكل كبير للمؤسسات بمختلف أحجامها، مما يوفر الحماية ضد العديد من التهديدات المحتملة. فهو يجمع بين المصادقة البيومترية والشبكات العصبية وآليات التشفير، مما يوفر سرعة عالية ومقاومة للهجمات وتكاليف نشر منخفضة، مما يجعله حلاً مثاليًا للمؤسسات ذات الميزانيات المحدودة.

## Литература المراجع والمصادر


1. П.П. Бескид, Т.М. Татарникова Криптографические Методы Защиты Информации – URL: http://elib.rshu.ru/files_books/pdf/img -504184120.pdf .
2. Tan M., Le Q. EfficientNetV2: Smaller Models and Faster Training //arXiv preprint, 2021.–URL: https://arxiv.org/pdf/2104.00298.