УДК 004.6:37

О. Я. Швец

доцент кафедры прикладной информатики,
и. о. декана факультета цифровых технологий,
канд. техн. наук, доцент
Новосибирский государственный университет экономики и управления
o.y.shvec@edu.nsuem.ru

Д. Ю. Кондратов

ассистент кафедры статистики
Новосибирский государственный университет экономики и управления
d.y.kondratov@edu.nsuem.ru

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ BIG DATA ДЛЯ МОНИТОРИНГА И ПРОГНОЗИРОВАНИЯ УГРОЗ В СИСТЕМАХ ДОПУСКА В ВУЗЫ И ШКОЛЫ

Статья посвящена разработке и внедрению интеллектуальной системы контроля и управления доступом (СКУД) в образовательных учреждениях на основе технологий Big Data. В работе рассматриваются архитектурные особенности системы, включая интеграцию видеоаналитики, электронных пропусков и датчиков мониторинга, а также анализируются технологические сложности обработки неструктурированной информации в реальном времени. Особое внимание уделено вопросам защиты персональных данных и минимизации ложноположительных срабатываний, что является критическим фактором надежности интеллектуальных систем. В качестве ключевых рекомендаций предлагается модульный подход к масштабированию инфраструктуры безопасности, ориентированный на повышение превентивной защиты образовательной среды. Предложенная модель рассматривается как часть цифровой трансформации образовательной инфраструктуры, обеспечивающая новый уровень безопасности при сохранении высокой пропускной способности.

Ключевые слова: Big Data, СКУД, предиктивная аналитика, безопасность образовательных учреждений, машинное обучение, интеллектуальные системы, мониторинг потоков

O. Y. Shvets

Associate Professor of the Department of Applied Informatics,
Acting Dean of the Faculty of Digital Technologies,
PhD of Technical Sciences, Associate Professor
Novosibirsk State University of Economics and Management
o.y.shvec@edu.nsuem.ru

D. Y. Kondratov

Assistant of the Department of Statistics
Novosibirsk State University of Economics and Management
d.y.kondratov@edu.nsuem.ru

APPLICATION OF BIG DATA TECHNOLOGIES FOR MONITORING AND FORECASTING THREATS IN UNIVERSITIES AND SCHOOLS ADMISSION SYSTEMS

The article is devoted to the development and implementation of an intelligent access control and management system (ACMS) in educational institutions based on Big Data technologies. The paper

discusses the architectural features of the system, including the integration of video analytics, electronic passes, and monitoring sensors, and analyzes the technological challenges of processing unstructured information in real time. Special attention is paid to the protection of personal data and the minimization of false positives, which is a critical factor in the reliability of intelligent systems. As key recommendations, a modular approach to scaling the security infrastructure is proposed, which is focused on improving the preventive protection of the educational environment. The proposed model is considered as part of the digital transformation of the educational infrastructure, providing a new level of security while maintaining high throughput.

Key words: Big Data, SCADA, predictive analytics, security of educational institutions, machine learning, intelligent systems, and flow monitoring

Современные образовательные учреждения сталкиваются с вызовом высокой динамики человеческих потоков, что требует кардинального пересмотра подходов к обеспечению безопасности. Традиционные системы контроля и управления доступом (СКУД), построенные на принципах жесткой верификации «один идентификатор — один доступ», сегодня функционируют исключительно реактивно: они фиксируют событие входа или выхода постфактум, без учета контекстной информации, что делает их критически уязвимыми перед лицом сложных, нетривиальных угроз. Переход к концепции Big Data подразумевает концептуальный отказ от использования разрозненных, изолированных баз данных в пользу создания единых распределенных информационных экосистем, способных к непрерывному интеллектуальному анализу [1].

Архитектура предлагаемой системы строится на четырех эшелонах, каждый из которых играет свою уникальную роль в цикле обеспечения безопасности [2]. На первом уровне — уровне первичного сбора данных (Data Ingestion) — происходит мультимодальный захват информации. Видеоаналитика, базирующаяся на глубоком обучении сверточных нейронных сетей, не только распознает лица в условиях различной освещенности, но и осуществляет детекцию подозрительных объектов, а также проводит анализ эмоционального фона толпы для раннего выявления признаков паники или агрессии. Данные с RFID-считывателей, биометрических терминалов и мобильных идентификаторов (NFC/Bluetooth) здесь дополняются телеметрией с датчиков контроля плотности потока, установленных в ключевых зонах входа, столовых и общих холлах.

Далее информация поступает на уровень потоковой обработки. Использование высокопроизводительных брокеров сообщений, таких как Apache Kafka, позволяет нивелировать задержки в передаче сигнала от периферийных датчиков к центральному ядру [3]. Информация от тысяч сенсоров агрегируется в режиме реального времени, что является фундаментальным требованием для предиктивного мониторинга, так как промедление в анализе событий на несколько секунд может быть критичным. Уровень хранения предполагает гибридный подход: структурированные логи, содержащие временные метки и идентификаторы, хранятся в реляционных БД для обеспечения быстрой выборки, в то время как массивы неструктурированных данных — видеопотоки, аудиофрагменты и журналы событий нейросетей — распределяются в кластерных хранилищах (типа Hadoop HDFS или S3-совместимых решений). Такая масштабируемость позволяет системе расти вместе с расширением кампуса.

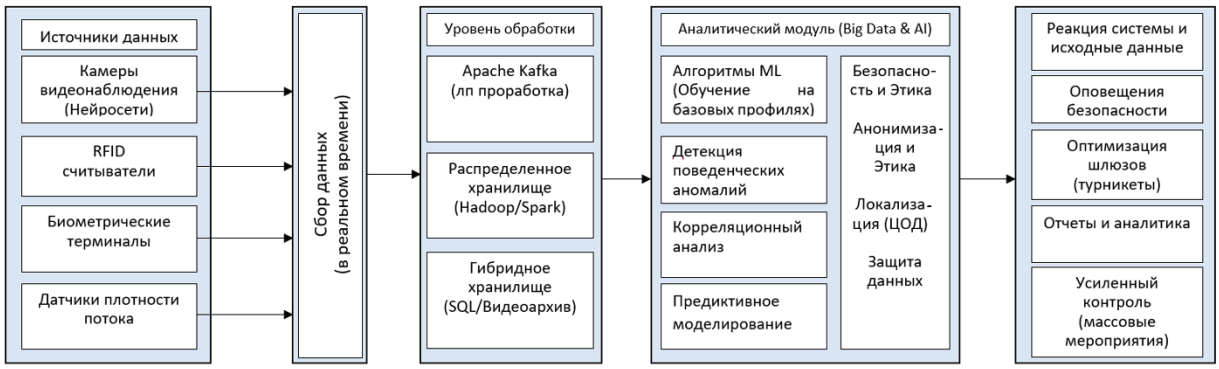
В аналитическом модуле разворачиваются сложные алгоритмы машинного обучения, которые проводят глубокий кластерный анализ перемещений. Система проходит стадию «обучения» на исторических данных в течение семестра, формируя матрицу типичного поведения для каждого сегмента пользователей — от студентов, имеющих доступ только в учебные аудитории, до преподавателей и административного персонала с расширенными правами. Основная ценность применения Big Data заключается в выявлении «скрытых» корреляций. Система способна обнаружить аномалии, абсолютно невидимые для оператора-человека: например, при поведенческом профилинге система соотносит маршрут пользователя

с его индивидуальным академическим расписанием; если студент, имеющий в это время лекцию, оказывается в административном крыле, уровень его «индекса риска» автоматически повышается. Также система осуществляет детекцию социальных аномалий путем анализа графов взаимодействия, отслеживая подозрительно длительные контакты с незнакомыми лицами в зонах ограниченного доступа. Предиктивное моделирование часов пик позволяет динамически перераспределять пропускную способность шлюзов, предотвращая скученность, которая признана экспертами одним из наиболее серьезных рисков безопасности [4].

Внедрение подобных систем в образовательную среду неизбежно требует строгого этического и юридического фреймворка, поэтому мы настаиваем на концепции локального суверенитета данных, где весь цикл обработки замыкается внутри защищенного контура университета (on-premise). Это полностью исключает зависимость от зарубежных облачных провайдеров и минимизирует риски компрометации данных, что критически важно в условиях текущей геополитической нестабильности и технологического противостояния [5]. Сравнение с существующими проприетарными решениями показывает, что классическая привязка к поставщику (vendor lock-in) существенно ограничивает возможности вуза по гибкой настройке безопасности, в то время как наша открытая архитектура позволяет адаптировать алгоритмы под меняющиеся нужды учреждения.

Экономическое обоснование такого внедрения выходит далеко за рамки простой автоматизации. Помимо оптимизации затрат на охранный персонал, система существенно снижает финансовые риски, связанные с последствиями инцидентов, стоимость устранения которых кратно превышает стоимость разработки локального ПО. Для обеспечения прозрачности процессов предлагается повсеместное внедрение анонимизированных хеш-идентификаторов для исследовательских нужд, а вся законодательная база должна быть подкреплена автоматизированными системами внутреннего аудита. Крайне важным аспектом остается развитие местных компетенций: вовлечение студентов ИТ-специальностей в обслуживание и развитие данных систем превращает вуз в заказчика и разработчика одновременно, замыкая цикл инноваций внутри научно-образовательной среды [6]. По аналогии с глобальными трендами на цифровой суверенитет, формирование вузовских стандартов доступа может стать региональным эталоном, способствуя гармонизации нормативных актов и укреплению общей защищенности образовательного пространства. Таким образом, переход к Big Data — это формирование новой управленческой парадигмы, где вуз выступает полноправным оператором своей цифровой среды, обеспечивая безопасность сообщества на базе собственных инновационных решений. Логическая блок-схема интеллектуальной системы контроля доступа на базе технологий Big Data для образовательных учреждений представлена на рисунке.

Логическая блок-схема интеллектуальной системы контроля доступа на базе технологий Big Data для образовательных учреждений



Логическая блок-схема интеллектуальной системы контроля доступа

Подводя итог проведенному исследованию, можно с уверенностью утверждать, что внедрение технологий Big Data в системы контроля и управления доступом (СКУД) образовательных учреждений представляет собой не просто техническую модернизацию, а необходимый переход к принципиально новой парадигме безопасности. Традиционные методы контроля, опирающиеся на статические алгоритмы идентификации, исчерпали свой потенциал в условиях возрастающей сложности образовательной среды. Предложенная нами модель, основанная на интеллектуальной обработке данных и предиктивной аналитике, демонстрирует, что переход от реактивного реагирования на инциденты к их заблаговременному прогнозированию является единственно эффективным способом обеспечения безопасности в динамично меняющихся условиях современных кампусов.

Преимущества использования Big Data в данной сфере охватывают целый комплекс аспектов: от качественного повышения уровня защищенности до формирования собственной технологической независимости вуза. Во-первых, интеллектуальный анализ данных в режиме реального времени позволяет системе не только распознавать субъектов, но и понимать контекст их поведения, выявляя скрытые аномалии и угрозы, которые недоступны для человеческого наблюдения. Это создает непрерывный контур мониторинга, адаптирующийся под специфические ритмы жизни учебного заведения. Во-вторых, переход к открытой архитектуре на базе Big Data освобождает образовательные учреждения от зависимости от проприетарных решений крупных иностранных вендоров, избавляя от проблемы «vendor lock-in». Это создает условия для реализации концепции «локального суверенитета данных», когда все процессы обработки информации остаются внутри защищенного контура университета, что критически важно для защиты персональных данных учащихся и сотрудников.

В экономической и управленческой перспективах данная система выступает как инструмент оптимизации. Предиктивное моделирование нагрузок не только предотвращает риски, связанные со скученностью людей в местах массового скопления, но и позволяет эффективно перераспределять ресурсы учреждения, снижая издержки на необоснованное содержание избыточного охранного персонала. Кроме того, реализация проекта дает мощный импульс для развития человеческого капитала: вовлечение студентов профильных ИТ-специальностей в разработку и поддержку подобных систем формирует уникальную кадровую базу, способную проектировать и развивать сложные технологические решения внутри научно-образовательной среды.

В конечном счете, безопасность в образовании перестает быть совокупностью ограничительных мер и «турникетов» — она трансформируется в предсказуемую, адаптивную и эффективную цифровую экосистему. В перспективе развитие данных решений в сторону интеграции с общегородскими цифровыми контурами позволит образовательным учреждениям органично встроиться в архитектуру «умного города», обеспечивая комплексную защиту при сохранении высокой пропускной способности и комфорта образовательного процесса. Таким образом, применение больших данных — это ключевой фактор формирования системы управления, основанной на доказательной аналитике, которая обеспечивает долгосрочную устойчивость и геополитическую значимость образовательной среды в условиях глобальной цифровизации. Данное исследование подтверждает, что будущее безопасности образовательных учреждений лежит на стыке фундаментальных научных подходов и инновационных цифровых технологий, управляемых непосредственно самим академическим сообществом.

Список литературы

1. Mayer-Schönberger, V., & Cukier, K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. URL: https://www.mann-ivanov-ferber.ru/assets/files/bookparts/bolshie-dannye/big_data_read.pdf (дата обращения: 03.03.2026).

2. Cloud Native Computing Foundation (CNCF). URL: https://architecture.cncf.io/ (дата обращения: 03.03.2026).
3. Confluent Documentation. Stream Processing for Real-time Monitoring. URL: https://docs.confluent.io/platform/current/streams/index.html (дата обращения: 03.03.2026).
4. ScienceDirect. Predictive analysis of crowd dynamics for safety in large-scale public environments. URL: https://www.sciencedirect.com/science/article/pii/S036013232200392X (дата обращения: 03.03.2026).
5. European Data Protection Board (EDPB). Guidelines on Data Protection in Smart Campus Environments. URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en (дата обращения: 03.03.2026).
6. The International Institute of Online Education Developmental Report (2019–2022) URL: https://ichei.org/en/news/activity/1816.html (дата обращения: 03.03.2026).