УДК 159.9:331.101.3 **DOI: 10.34670/AR.2026.74.97.001**

Интеллектуальная система комплексного мониторинга безопасности образовательной организации на основе ансамбля нейросетевых моделей

Сосковец Альберт Владимирович

Старший преподаватель,
Омский государственный технический университет,
644050, Российская Федерация, Омск, просп. Мира, 11;
e-mail: soskovets.albert@mail.ru

Шельтик Кристина Георгиевна

Аспирант,
Омский государственный технический университет,
644050, Российская Федерация, Омск, просп. Мира, 11;
e-mail: rodispublishing@yandex.ru

Воронцов Илья Сергеевич

Магистрант,
Омский государственный технический университет,
644050, Российская Федерация, Омск, просп. Мира, 11;
e-mail: analitikarodis@yandex.ru

Аннотация

В статье обосновывается актуальность создания интеллектуальных систем обеспечения безопасности для образовательных организаций, выступающих в качестве объектов массового пребывания людей с высоким уровнем социальной интерактивности. Целью исследования является разработка архитектуры подсистемы комплексного мониторинга, способной в реальном времени оценивать интегральный риск нарушения безопасности на основе анализа гетерогенных данных. Новизна предлагаемого подхода заключается в конвергенции трех аналитических контуров: 1) контура выявления технических аномалий на основе нейросетевых автоэнкодеров (NAE) и методов обнаружения выбросов (LOF); 2) контура анализа поведенческих и психофизиологических характеристик субъектов с применением гибридных нейросетевых моделей (CNN + LSTM) для распознавания эмоций (FER) и классификации аномальных действий; 3) контура корреляции событий на основе модели совместного обнаружения аномалий (JADM). Особое внимание уделяется концепции «персонального ассистента» — специализированной нейросетевой модели, аккумулирующей данные конкретного субъекта со смарт-часов и систем видеонаблюдения для повышения точности идентификации девиантного поведения. Предложенная архитектура позволяет перейти от реактивного реагирования на инциденты к проактивному управлению рисками на основе непрерывного интеллектуального анализа ситуации в каждой зоне контроля.

Для цитирования в научных исследованиях

Сосковец А.В., Шельтик К.Г., Воронцов И.С. Интеллектуальная система комплексного мониторинга безопасности образовательной организации на основе ансамбля нейросетевых моделей // Психология. Историко-критические обзоры и современные исследования. 2026. Т. 15. № 1А. С. 160-169. DOI: 10.34670/AR.2026.74.97.001

Ключевые слова

Комплексная безопасность образовательной организации, интеллектуальный мониторинг, обнаружение аномалий, нейросетевой автоэнкодер (NAE), распознавание эмоций (FER), сверточные нейронные сети (CNN), сеть долгой краткосрочной памяти (LSTM), изолирующий лес (IFO), модель совместного обнаружения аномалий (JADM), персональный ассистент, проактивное управление рисками, машинное обучение.

Введение

Современные образовательные организации представляют собой сложные социотехнические системы, характеризующиеся высокой плотностью потоков людей, разнообразием используемого оборудования и открытостью среды для внешних взаимодействий. Анализ резонансных происшествий последних лет, включая трагические события в местах массового скопления людей [Теракт в «Крокус Сити Холле», 2024, www…], свидетельствует о наличии системных уязвимостей в существующих подходах к обеспечению безопасности. Традиционные системы, основанные на разрозненном функционировании средств охраны, пожарной сигнализации и видеонаблюдения, не способны формировать целостную картину развития угрозы, особенно если она носит комплексный характер и инициируется легитимными пользователями пространства.

Цифровая трансформация образовательной среды создает предпосылки для качественного изменения парадигмы безопасности – перехода от пассивной фиксации нарушений к проактивному мониторингу и прогнозированию рисков. Это становится возможным благодаря интеграции в единый контур управления данных от традиционных сенсоров, систем видеонаблюдения и, что особенно важно, носимых устройств (смарт-часов, браслетов), которые уже активно используются участниками образовательного процесса. Возникает задача разработки методов интеллектуального анализа этого гетерогенного потока данных для своевременного выявления как технических неисправностей, так и поведенческих аномалий, потенциально ведущих к нарушению безопасности.

Целью настоящей работы является теоретическое обоснование и описание архитектуры интеллектуальной подсистемы комплексного мониторинга безопасности образовательной организации, основанной на ансамблевом использовании моделей машинного обучения и реализующей концепцию персональных ассистентов для каждого субъекта, находящегося в зоне контроля.

Современное состояние проблемы и обоснование необходимости комплексного подхода

Задача обеспечения безопасности образовательной среды носит многокритериальный характер. Как отмечается в [Проталинский, Ажмухамедов, 2012; Аникин, Емалетдинова, Кирпичников, 2015], оценка рисков требует учета широкого спектра показателей: от

финансовых потерь и репутационных издержек до прямой угрозы жизни и здоровью участников образовательного процесса. При этом классические методы риск-менеджмента, базирующиеся на периодических экспертных оценках, обладают рядом недостатков. Во-первых, они субъективны и зависят от квалификации и опыта конкретных экспертов [Абрамова, 2007]. Во-вторых, они дискретны и не способны отражать динамику изменений операционной обстановки. В-третьих, решения в различных контурах безопасности (информационная, физическая, пожарная) часто принимаются изолированно, без согласования между собой и с рядовыми сотрудниками, которые являются конечными исполнителями предписаний [Зубарев, 2022].

Современные исследования в области безопасности объектов критической информационной инфраструктуры указывают на необходимость консолидации данных из множества источников для обеспечения контекста потенциальной атаки [Вульфин, 2023]. Применение методов компьютерного зрения, управляемых искусственным интеллектом, уже доказало свою эффективность в задачах классификации и детекции [Хлудов, 2023; Перекопновский, 2023]. Однако перенос этих подходов на образовательную среду требует учета ее специфики: необходимо понимание не только факта присутствия объекта, но и семантики действий субъекта, его эмоционального и физического состояния.

Таким образом, возникает потребность в создании такой системы мониторинга, которая бы непрерывно агрегировала и анализировала данные о состоянии технических подсистем (телеметрия) и поведении людей (видеоряд, биометрические показатели), преобразуя их в многомерные временные ряды для последующего интеллектуального анализа. Это позволит не только фиксировать очевидные нарушения, но и выявлять латентные угрозы на ранней стадии их развития.

Математическая формализация задачи мониторинга

Представим образовательную организацию как множество пространственных зон наблюдения $Z=\{z1,z2,...,zn\}$. Для каждой зоны zi в дискретные моменты времени $t \in T$ формируется массив гетерогенных данных, поступающих от трех основных источников:

1. Множество технических сенсоров $C=\{c1,c2,...,ck\}$, формирующих телеметрические временные ряды.
2. Множество видеокамер $V=\{v1,v2,...,vm\}$, генерирующих непрерывный видеопоток.
3. Множество персональных носимых устройств (смарт-часов) $W=\{w1,w2,...,wp\}$, принадлежащих субъектам, находящимся в зоне zi.

Состояние зоны zi в момент времени t описывается кортежем:

$Di(t)=\{SC(t),SV(t),SW(t)\}$

где SC(t) – нормализованные показания сенсоров, преобразованные в многомерный телеметрический временной ряд (МТВР); SV(t)– множество сегментов видеоданных; SW(t) – структурированные данные со смарт-часов (идентификатор субъекта, пульс, локальные перемещения и пр.).

Целью функционирования системы является вычисление интегрального показателя риска Ri(t) для каждой зоны, представляющего собой функцию от анализа всех доступных данных:

$Ri(t)=F(Di(t))$

Задача синтеза заключается в нахождении такого оператора F*F* (ансамбля моделей ИИ), который минимизировал бы ошибку прогноза между рассчитанным уровнем риска и фактом реализации угрозы безопасности в зоне *zi*.

Архитектура системы интеллектуального комплексного мониторинга

Предлагаемая архитектура реализует оператор F*F* через трехуровневую иерархию обработки данных, включающую параллельное функционирование двух аналитических контуров и их последующую интеграцию (рис. 1).

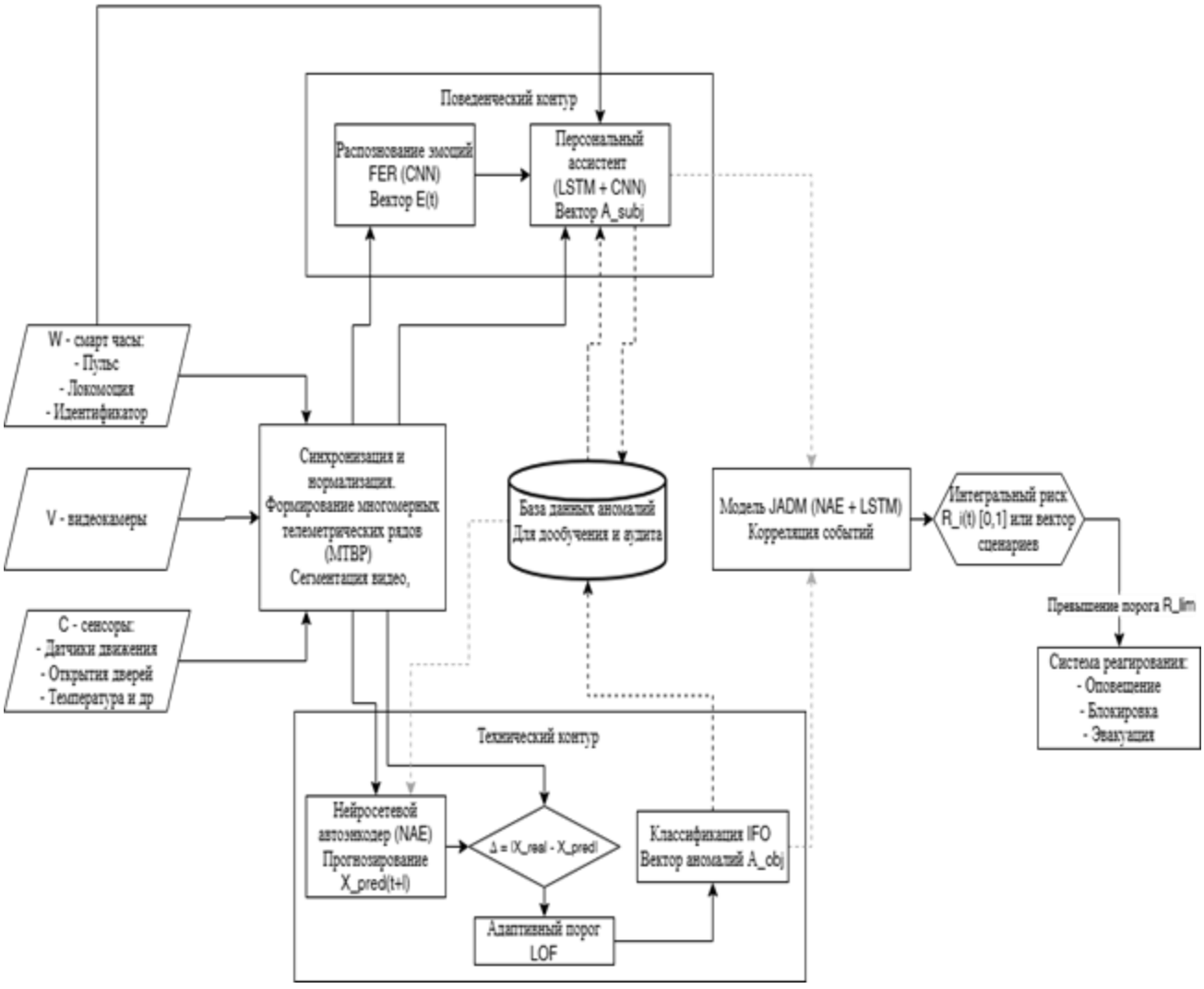

Рисунок 1 – Архитектура системы интеллектуального комплексного мониторинга

Уровень сбора и первичной обработки данных

На этом уровне осуществляется синхронизация потоков данных по времени. Данные с сенсоров SC(t) проходят фильтрацию шумов и нормализацию, после чего формируются в многомерный временной ряд X(t). Видеопоток SV(t) сегментируется на интервалы фиксированной длины (например, по 64 кадра). Данные со смарт-часов SW(t) верифицируются

и привязываются к конкретным субъектам, идентифицированным в зоне. Для технических систем состав источников C и V в зоне постоянен, тогда как множество субъектов W является динамическим.

Контур анализа технических аномалий (объектный уровень)

Для обнаружения отклонений в работе технических систем и появления посторонних объектов используется метод, основанный на способности нейросетевых моделей к прогнозированию «нормального» поведения.

Нейросетевой автоэнкодер (NAE) для прогнозирования временных рядов

Основой контура является многомерный автоэнкодер (NAE), обучаемый на множестве эталонных фрагментов временных рядов Xtrain. Задача NAE – реконструкция (прогнозирование) поведения системы на l временных окон вперед:

$X^{(t+l)}=NAE(X(t),X(t-1),...,X(t-h))$

где h – глубина исторического окна. В процессе функционирования NAE генерирует прогнозируемое моделируемое окно данных X^win для каждого интервала наблюдения.

Детекция и классификация аномалий

Модуль сравнения принимает реальные данные окна Xwin и прогнозируемые X^win, вычисляя ошибку реконструкции (разность панорам). Для минимизации ложных срабатываний используется адаптивный порог θ, который динамически пересчитывается на основе статистических характеристик данных. Эффективным инструментом для этого является модель локального уровня выбросов LOF (Local Outlier Factor) [Breunig, Kröger, Ng, Sander, 2000], которая оценивает локальное отклонение плотности точек данных.

Точки данных, для которых ошибка реконструкции превышает порог θ, формируют матрицу потенциальных аномалий Mobj. Для классификации типа аномалии и получения вектора ее признаков Aobj применяется ансамбль детекторов на основе метода изолирующего леса IFO (Isolation Forest) [Ананьев, 2020]. IFO эффективно обрабатывает многомерные данные, изолируя аномалии путем случайного разбиения пространства признаков. На выходе контура формируется множество верифицированных технических аномалий {Aobj1, Aobj2, ...} для каждой зоны zi.

Контур анализа поведенческих и психофизиологических аномалий (субъектный уровень)

Этот контур предназначен для оценки состояния людей, находящихся в зоне мониторинга. Его ключевая особенность – создание для каждого субъекта «персонального ассистента», модели, анализирующей динамику его поведения.

Распознавание эмоционального состояния

Сегменты видеоданных SV(t) для каждого субъекта поступают в модуль распознавания эмоций FER (Facial Emotion Recognition) на основе сверточных нейронных сетей (CNN) [Рюмина, Карпов, 2020]. Модель FER выделяет ключевые точки лица и классифицирует базовые эмоции, формируя вектор эмоционального состояния E(t). В контексте задач безопасности в качестве критических (аномальных) рассматриваются состояния, классифицируемые как «гнев» и «печаль», которые могут свидетельствовать о высоком уровне фрустрации или агрессии.

Анализ действий и физиологического состояния

Данные со смарт-часов wj (вариабельность сердечного ритма, акселерометрия) синхронизируются с видеорядом и результатами работы FER. Совокупность этих данных (поза, перемещения, эмоция, пульс) подается на вход «персонального ассистента» – гибридной нейросетевой модели.

Для учета временной динамики поведения используется рекуррентная нейронная сеть (RNN), в частности сеть долгой краткосрочной памяти (LSTM) архитектуры «многие ко

многим». LSTM моделирует эволюцию поведенческих признаков во времени. Однако для сохранения пространственно-временной информации (например, специфической позы или взаимодействия с предметом) на втором уровне внимания применяется сверточная нейронная сеть (CNN), которая агрегирует выходные векторы LSTM. Это позволяет модели распознавать сложные поведенческие паттерны: наличие оружия, нехарактерную траекторию движения, имитацию правомерных действий с противоправной целью.

Обучение персональных ассистентов производится на комбинации данных с размеченных датасетов, таких как UCF-Crime [Park, Kim, Han, 2021], содержащих примеры как нормального, так и аномального поведения (драки, кражи, стрельба). На выходе контура для каждого субъекта j формируется вектор поведенческих аномалий Asubjj (например, «агрессивная жестикуляция», «нахождение в запретной зоне», «критическое изменение пульса»). Совокупность таких векторов для зоны zi образует множество {Asubj}.

Уровень корреляции и интегральной оценки риска

На этом уровне происходит объединение результатов работы объектного и субъектного контуров с целью выявления комплексных угроз, которые не фиксируются каждым из контуров по отдельности.

Модель совместного обнаружения аномалий (JADM)

Модель совместного обнаружения аномалий JADM (Joint Anomaly Detection Model) [Salazar, Conde, Irazábal, Vicente, 2021; Mao, Ding, Liu, et al., 2021] получает на вход за временной интервал [t,t+Δ] множество технических аномалий {Aobj} и множество поведенческих аномалий {Asubj} для зоны zi. JADM реализована на основе еще одного ансамбля нейросетевых автоэнкодеров с LSTM-слоями. Ее задача – найти корреляции между, казалось бы, разрозненными событиями. Например:

– Событие 1 (техническое): Отказ работы датчика двери в запасном выходе.
– Событие 2 (поведенческое): Двое субъектов демонстрируют низкую вариабельность сердечного ритма и сфокусированное внимание на одном объекте.
– Событие 3 (поведенческое): Третий субъект проявляет эмоцию страха.

По отдельности эти события могут быть проигнорированы как ложные или малозначимые. Однако JADM, обученная на сценариях развития комплексных атак, может выявить их взаимосвязь и классифицировать ситуацию как подготовку к несанкционированному проникновению или иному нарушению.

Формирование интегральной оценки риска

Выходом модели JADM является интегральная оценка риска Ri(t) для зоны контроля. Оценка может быть представлена как:

– скалярное значение в диапазоне [0, 1], где 1 – критический уровень риска;
– вектор вероятностей [P1,P2,...,Pk] реализации каждого из k сценариев угроз (пожар, несанкционированное проникновение, агрессия, террористический акт).

Превышение интегральной оценкой заданного порога Rlim или высокая вероятность критического сценария инициирует процесс принятия решений: оповещение службы безопасности, блокирование зон, запуск протоколов эвакуации и т.д.

Заключение

Разработка и внедрение систем комплексного интеллектуального мониторинга является необходимым условием для обеспечения безопасности современных образовательных

организаций. Предложенная в работе архитектура позволяет преодолеть ограничения традиционных систем за счет конвергенции данных из разнородных источников и применения ансамбля специализированных моделей искусственного интеллекта.

Ключевой научный результат исследования заключается в обосновании метода синергетического использования нейросетевых автоэнкодеров (NAE), детекторов на основе изолирующего леса (IFO), моделей распознавания эмоций (FER) и моделей совместного обнаружения аномалий (JADM). Это позволяет в реальном времени оценивать не только текущие отклонения в работе технических систем, но и прогнозировать поведенческие риски на основе анализа эмоционального и физиологического состояния субъектов, реализуя тем самым концепцию «персонального ассистента».

Практическая значимость работы состоит в создании теоретического базиса для разработки программного обеспечения, интегрируемого в существующую инфраструктуру безопасности образовательных организаций. Дальнейшие исследования будут направлены на разработку методик обучения предложенного ансамбля моделей, адаптацию существующих датасетов (например, UCF-Crime) к специфике образовательной среды и экспериментальную апробацию системы на базе университетского кампуса.

Библиография

1. Абрамова, Н. А. О проблеме рисков из-за человеческого фактора в экспертных методах и информационных технологиях / Н. А. Абрамова // Проблемы управления. — 2007. — № 2. — С. 11-21.
2. Ананьев, А. А. Использование алгоритма isolation forest для решения задачи обнаружения аномалий в работе микропроцессорных пластиковых карт / А. А. Ананьев // Информатизация и связь. — 2020. — № 3. — С. 26-30. DOI 10.34219/2078-8320-2020-11-3-26-30.
3. Аникин, И. В. Методы оценки и управления рисками информационной безопасности в корпоративных информационных сетях / И. В. Аникин, Л. Ю. Емалетдинова, А. П. Кирпичников // Вестник Технологического университета. — 2015. — Т. 18, № 6. — С. 195-197.
4. Антохина, Ю. А. Особенности организационной структуры управления на различных этапах жизненного цикла образовательной организации / Ю. А. Антохина, А. М. Колесников, Е. М. Храповицкая // Вестник экономической безопасности. — 2016. — № 2. — С. 275-280.
5. Васильев, В. И. Обеспечение информационной безопасности киберфизических объектов на основе прогнозирования и обнаружения аномалий их состояния / В. И. Васильев [и др.] // Системы управления, связи и безопасности. — 2021. — № 6. — С. 90-119. — DOI 10.24412/2410-9916-2021-6-90-119.
6. Вульфин, А. М. Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных / А. М. Вульфин // Системная инженерия и информационные технологии. — 2023. — Т. 5, № 4(13). — С. 50-76. — DOI 10.54708/2658-5014-SIIT-2023-no3-p50.
7. Зубарев, Н. Ю. Анализ факторов, влияющих на реализацию инноваций в научно-технических разработках университета / Н. Ю. Зубарев // Вестник евразийской науки. — 2022. — Т. 14, № 6.
8. Перекопновский, Д. И. Применение компьютерного зрения и искусственного интеллекта в современном мире / Д. И. Перекопновский // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации : сборник статей LXXIII Международной научно-практической конференции. — Уфа: НИЦ «Вестник науки», 2023. — С. 262-265.
9. Проталинский, О. М. Системный анализ и моделирование слабо структурированных и плохо формализуемых процессов в социотехнических системах / О. М. Проталинский, И. М. Ажмухамедов // Инженерный вестник Дона. — 2012. — № 3(21). — С. 179-187.
10. Рюмина, Е. В. Аналитический обзор методов распознавания эмоций по выражениям лица человека / Е. В. Рюмина, А. А. Карпов // Научно-технический вестник информационных технологий, механики и оптики. — 2020. — Т. 20, № 2. — С. 163-176. — DOI 10.17586/2226-1494-2020-20-2-163-176.
11. Теракт в «Крокус Сити Холле» // Википедия. Свободная энциклопедия. — URL: https://ru.wikipedia.org/wiki/Теракт_в_«Крокус_Сити_Холле» (дата обращения: 20.04.2024).
12. Хлудов, И. В. Компьютерное зрение и его применение в медицине, автономных автомобилях и других областях / И. В. Хлудов // Актуальные исследования. — 2023. — № 30(160). — С. 17-19.

13. Breunig, M. LOF: Identifying Density-Based Local Outliers / M. Breunig, P. Kröger, R. Ng, J. Sander // ACM Sigmod Record. — 2000. — Vol. 29. — P. 93-104. — DOI 10.1145/342009.335388.
14. Mao, W. A new deep domain adaptation method with joint adversarial training for online detection of bearing early fault / W. Mao, L. Ding, Y. Liu [et al.] // ISA Transactions. — 2021. — DOI 10.1016/j.isatra.2021.04.026.
15. Park, J. Learning to Adapt to Unseen Abnormal Activities Under Weak Supervision / J. Park, J. Kim, B. Han // Lecture Notes in Computer Science. — 2021. — Vol. 12626 LNCS. — P. 514-529. — DOI 10.1007/978-3-030-69541-5_31.
16. Salazar, F. Anomaly detection in dam behaviour with machine learning classification models / F. Salazar, A. Conde, J. Irazábal, D. J. Vicente // Water. — 2021. — Vol. 13, No. 17. — DOI 10.3390/w13172387.

Intelligent System for Integrated Security Monitoring of an Educational Organization Based on an Ensemble of Neural Network Models

Al'bert V. Soskovets

Senior Lecturer,
Omsk State Technical University,
644050, 11, Mira ave., Omsk, Russian Federation;
e-mail: soskovets.albert@mail.ru

Kristina G. Shel'tik

Postgraduate Student,
Omsk State Technical University,
644050, 11, Mira ave., Omsk, Russian Federation;
e-mail: rodispublishing@yandex.ru

Il'ya S. Vorontsov

Master's Student,
Omsk State Technical University,
644050, 11, Mira ave., Omsk, Russian Federation;
e-mail: analitikarodis@yandex.ru

Abstract

The article substantiates the relevance of creating intelligent security systems for educational organizations, which serve as sites of mass gathering of people with a high level of social interactivity. The aim of the study is to develop an architecture for an integrated monitoring subsystem capable of assessing in real time the integral security risk based on the analysis of heterogeneous data. The novelty of the proposed approach lies in the convergence of three analytical contours: 1) a contour for identifying technical anomalies based on neural network autoencoders (NAE) and outlier detection methods (LOF); 2) a contour for analyzing behavioral and psychophysiological characteristics of subjects using hybrid neural network models (CNN + LSTM) for emotion recognition (FER) and classification of anomalous actions; 3) an event correlation contour based on a joint anomaly detection model (JADM). Special attention is paid to the concept of a "personal assistant" — a specialized neural network model that accumulates data of a specific

subject from smartwatches and video surveillance systems to improve the accuracy of identifying deviant behavior. The proposed architecture allows for a transition from reactive incident response to proactive risk management based on continuous intelligent analysis of the situation in each control zone.

For citation

Soskovets A.V., Shel'tik K.G., Vorontsov I.S. (2026) Intellektual'naya sistema kompleksnogo monitoringa bezopasnosti obrazovatel'noy organizatsii na osnove ansamblya neyrosetevykh modeley [Intelligent System for Integrated Security Monitoring of an Educational Organization Based on an Ensemble of Neural Network Models]. *Psikhologiya. Istoriko-kriticheskie obzory i sovremennye issledovaniya* [Psychology. Historical-critical Reviews and Current Researches], 15 (1A), pp. 160-169. DOI: 10.34670/AR.2026.74.97.001

Keywords

Integrated security of an educational organization, intelligent monitoring, anomaly detection, neural network autoencoder (NAE), emotion recognition (FER), convolutional neural networks (CNN), long short-term memory (LSTM), isolation forest (IFO), joint anomaly detection model (JADM), personal assistant, proactive risk management, machine learning.

References

1. Abramova, N. A. (2007). O probleme riskov iz-za chelovecheskogo faktora v ekspertnykh metodakh i informatsionnykh tekhnologiyakh [On the problem of risks due to human factor in expert methods and information technologies]. *Problemy upravleniya*, (2), 11-21.
2. Ananiev, A. A. (2020). Ispolzovanie algoritma isolation forest dlya resheniya zadachi obnaruzheniya anomaliy v rabote mikroprotsessornykh plastikovykh kart [Using the isolation forest algorithm to solve the problem of detecting anomalies in the operation of microprocessor plastic cards]. *Informatizatsiya i svyaz*, (3), 26-30. https://doi.org/10.34219/2078-8320-2020-11-3-26-30
3. Anikin, I. V., Emaletdinova, L. Y., & Kirpichnikov, A. P. (2015). Metody otsenki i upravleniya riskami informatsionnoy bezopasnosti v korporativnykh informatsionnykh setyakh [Methods for assessing and managing information security risks in corporate information networks]. *Vestnik Tekhnologicheskogo universiteta*, *18*(6), 195-197.
4. Antokhina, Y. A., Kolesnikov, A. M., & Khrapovitskaya, E. M. (2016). Osobennosti organizatsionnoy struktury upravleniya na razlichnykh etapakh zhiznennogo tsikla obrazovatelnoy organizatsii [Features of the organizational management structure at various stages of the life cycle of an educational organization]. *Vestnik ekonomicheskoy bezopasnosti*, (2), 275-280.
5. Breunig, M., Kröger, P., Ng, R., & Sander, J. (2000). LOF: Identifying density-based local outliers. *ACM Sigmod Record*, *29*, 93-104. https://doi.org/10.1145/342009.335388
6. Khludov, I. V. (2023). Kompyuternoe zrenie i ego primenenie v meditsine, avtonomnykh avtomobilyakh i drugikh oblastyakh [Computer vision and its application in medicine, autonomous cars and other fields]. *Aktualnye issledovaniya*, (30(160)), 17-19.
7. Mao, W., Ding, L., Liu, Y., [et al.]. (2021). A new deep domain adaptation method with joint adversarial training for online detection of bearing early fault. *ISA Transactions*. https://doi.org/10.1016/j.isatra.2021.04.026
8. Park, J., Kim, J., & Han, B. (2021). Learning to adapt to unseen abnormal activities under weak supervision. *Lecture Notes in Computer Science*, *12626*, 514-529. https://doi.org/10.1007/978-3-030-69541-5_31
9. Perekopnovskiy, D. I. (2023). Primenenie kompyuternogo zreniya i iskusstvennogo intellekta v sovremennom mire [Application of computer vision and artificial intelligence in the modern world]. In *Fundamentalnye i prikladnye nauchnye issledovaniya: aktualnye voprosy, dostizheniya i innovatsii* (pp. 262-265). NIC "Vestnik nauki".
10. Protalinskiy, O. M., & Azhmukhamedov, I. M. (2012). Sistemnyy analiz i modelirovanie slabo strukturirovannykh i plokho formalizuemykh protsessov v sotsiotekhnicheskikh sistemakh [System analysis and modeling of semi-structured and poorly formalized processes in socio-technical systems]. *Inzhenernyy vestnik Dona*, (3(21)), 179-187.
11. Ryumina, E. V., & Karpov, A. A. (2020). Analiticheskiy obzor metodov raspoznavaniya emotsiy po vyrazheniyam litsa cheloveka [Analytical review of emotion recognition methods from facial expressions]. *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki*, *20*(2), 163-176. https://doi.org/10.17586/2226-1494-2020-20-2-163-176

12. Salazar, F., Conde, A., Irazábal, J., & Vicente, D. J. (2021). Anomaly detection in dam behaviour with machine learning classification models. *Water*, *13*(17). https://doi.org/10.3390/w13172387
13. Terakt v "Krokus Siti Kholle" [Terrorist attack at Crocus City Hall]. (2024). In *Wikipedia*. Retrieved April 20, 2024, from https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%80%D0%B0%D0%BA%D1%82_%D0%B2_%C2%AB%D0%9A%D1%80%D0%BE%D0%BA%D1%83%D1%81_%D0%A1%D0%B8%D1%82%D0%B8_%D0%A5%D0%BE%D0%BB%D0%BB%D0%B5%C2%BB
14. Vasilyev, V. I., [et al.]. (2021). Obespechenie informatsionnoy bezopasnosti kiberfizicheskikh ob'ektov na osnove prognozirovaniya i obnaruzheniya anomaliy ikh sostoyaniya [Ensuring information security of cyber-physical objects based on forecasting and detecting anomalies of their state]. *Sistemy upravleniya, svyazi i bezopasnosti*, (6), 90-119. https://doi.org/10.24412/2410-9916-2021-6-90-119
15. Vulfin, A. M. (2023). Modeli i metody kompleksnoy otsenki riskov bezopasnosti ob'ektov kriticheskoy informatsionnoy infrastruktury na osnove intellektualnogo analiza dannykh [Models and methods for comprehensive security risk assessment of critical information infrastructure objects based on intelligent data analysis]. *Sistemnaya inzheneriya i informatsionnye tekhnologii*, *5*(4(13)), 50-76. https://doi.org/10.54708/2658-5014-SIIT-2023-no3-p50
16. Zubarev, N. Y. (2022). Analiz faktorov, vliyayushchikh na realizatsiyu innovatsiy v nauchno-tekhnicheskikh razrabotkakh universiteta [Analysis of factors influencing the implementation of innovations in scientific and technical developments of the university]. *Vestnik evraziyskoy nauki*, *14*(6).