Мир науки. Педагогика и психология / World of Science. Pedagogy and psychology https://mir-nauki.com

2024, Том 12, № 3 / 2024, Vol. 12, Iss. 3 https://mir-nauki.com/issue-3-2024.html

URL статьи: https://mir-nauki.com/PDF/76PSMN324.pdf

5.12.1. Междисциплинарные исследования когнитивных процессов (психологические науки)

Ссылка для цитирования этой статьи:
Сосковец, А. В. Обеспечение комплексной безопасности образовательной организации на основе интеллектуального мониторинга / А. В. Сосковец, Т. П. Мильчарек // Мир науки. Педагогика и психология. — 2024. — Т. 12. — № 3. — URL: https://mir-nauki.com/PDF/76PSMN324.pdf

For citation:
Soskovets A.V., Milczarek T.P. Ensuring comprehensive security of an educational organization based on intelligent monitoring. *World of Science. Pedagogy and psychology*. 2024;12(3): 76PSMN324. Available at: https://mir-nauki.com/PDF/76PSMN324.pdf. (In Russ., abstract in Eng.)

УДК 004.81

Сосковец Альберт Владимирович
ФГАОУ ВО «Омский государственный технический университет», Омск, Россия
Старший преподаватель кафедры «Психологии труда и организационной психологии»
E-mail: soskovets.albert@mail.ru
ORCID: https://orcid.org/0009-0003-2542-2592

Мильчарек Тадэуш Петрович
ФГАОУ ВО «Омский государственный технический университет», Омск, Россия
Заведующий кафедрой «Психологии труда и организационной психологии»
Кандидат философских наук, доцент

Обеспечение комплексной безопасности образовательной организации на основе интеллектуального мониторинга

Аннотация. В рамках исследования обоснована необходимость внедрения на объекты образовательных организаций интеллектуальной подсистемы комплексного мониторинга, позволяющей оценить комплексный риск нарушения ее безопасности. Предложена реализация данной подсистемы на основе применения ансамбля моделей искусственного интеллекта, осуществляющего выявление аномального поведения как объектов, так и субъектов в зоне наблюдения. Новизна предлагаемой модели состоит в том, что для повышения точности распознавания поведенческих аномалий субъектов используются модели распознавания эмоций FER на основе сверточных нейронных сетей CNN, модели анализа персональных характеристик здоровья субъектов на основе их считывания данных со смарт-часов. Совокупность данных моделей образуют множество персональных ассистентов. С целью повышения точности оценки комплексного риска используются модели корреляции аномалий JADM.

Ключевые слова: интеллектуальный мониторинг; детекторы аномалий; модели распознавания эмоций FER; нейросетевой автоэнкодер с долгой краткосрочной памятью; персональный ассистент; CNN

Введение

В результате террористического акта в «Крокус Сити Холле», произошедшего 22 марта 2024 года, в рамках которого было осуществлено нападение на концертный зал, погибли не

менее 145 человек.[1] Анализ данного события показал уязвимости как в системе мониторинга, так и в системе обеспечения безопасности граждан. Данный факт говорит о том, что угрозы нарушения безопасности объектов массового скопления людей в настоящее время остаются актуальными. Одним из видов таких объектов являются объекты образовательных организаций, которые также подвергались нападениям террористических групп ранее. Исходя из этого следует, что требуется разработка интеллектуальной подсистемы мониторинга, непрерывно осуществляющей анализ процессов, протекающих при осуществлении образовательной деятельности, а также количественно оценивающей уровень комплексного риска для каждой зоны наблюдения. Данная оценка в свою очередь позволит оценить защищенность процессов в полисубъектной среде, как в текущий момент времени, так и в будущем при соответствующем управлении рисками с целью формирования контрмер. В виду цифровизации как образовательного процесса, так и реализуемой системы охраны, на первое место по важности выходят информационные риски. Исходя из этого был проведен анализ методов оценки информационных рисков на предмет их полноты.

Анализ реализации процесса оценки информационных рисков

Авторы в [1] утверждают, что особенность системы риск-менеджмента в области информационных технологий и информационной безопасности заключается в том, что, она не может существовать отдельно и должна быть интегрирована в общую систему управления предприятия, а соответственно и в образовательную среду. Тем не менее интеллектуальные системы, отвечающие за безопасность, в настоящее время автоматизированным способом осуществляют семантический анализ данных, протекающих только внутри информационной системы, и не учитывают накапливаемые с помощью средств мониторинга данные внешней среды о субъектах и объектах в процессе образовательной деятельности. Кроме того, также можно сделать вывод, что реальное осуществление решения задачи обеспечения безопасности образовательной среды комплексно не осуществляется в виду того, что чаще всего эксперты в каждой области безопасности согласуют свое мнение только с руководителем и не согласуют его ни между собой, ни с сотрудниками, которые в последствии будут выполнять их предписания при выполнении своих должностных обязанностей.

Если рассматривать задачу оценки рисков с формальной точки зрения, то она является многокритериальной. С целью оценки ценности активов и значений ущерба используются следующие показатели: потеря репутации, безопасность сотрудников, финансовые потери, нестабильность функционирования и т. д. [2]. При этом для решения данной задачи требуется построить иерархию показателей и провести их ранжирование по уровням важности. Проведение данного процесса имеет субъективный характер в виду того, что в нем принимает участие множество экспертов [3]. При этом получаемый в результате оценки уровень риска является непостоянной величиной. В зависимости от изменений в процессах функционирования организации его необходимо постоянно пересчитывать и сравнивать со значением, которое является приемлемым для руководителя.

В зависимости от точности и своевременности оценки рисков в условиях возникновения плановых или непредвиденных событий, или обстоятельств, воздействующих на достижение целей организации (например, нехватка ресурсов, недостаточная компетентность, временные рамки и т. д.) можно оценить эффективность деятельности руководителя образовательной организации [4]. Обязательным условием успешного риск-менеджмента является его непрерывность.

[1] Теракт в «Крокус Сити Холле». Википедия. Свободная энциклопедия: [сайт]. — URL: https://ru.wikipedia.org/wiki/Теракт_в_«Крокус_Сити_Холле» (дата обращения: 20.04.2024).

С целью реализации непрерывной оценки рисков подсистему интеллектуального мониторинга необходимо интегрировать в систему управления образовательной организации, а также в жизненный цикл протекающих в ней процессов [5]. Функционирование данной подсистемы предлагается осуществить на основе компьютерного зрения, управляемого моделью искусственного интеллекта, так как успешность решения задачи классификации данным методом уже доказана и апробирована в разных сферах применения [6; 7]. Кроме того, использование сотрудниками и обучаемыми ВУЗа смарт-часов с модулем NFC позволит без внедрения дорогостоящего оборудования в режиме реального времени контролировать не только доступ на различные зоны ВУЗа, но и определять текущие физические показатели.

В рамках исследования [8] с целью анализа сценариев реализации угроз с возможностью приоритезации мер по их устранению необходимо обеспечение видимости и контекста потенциальной атаки за счет агрегации и анализа данных из множества источников, характеризующих состояние подсистем объекта КИИ. Если рассматривать в качестве объекта защиты образовательную организацию, то подсистема комплексного мониторинга должна понимать семантику действий не только объектов, но и субъектов на основе их поведения. Таким образом, если взять предложенную в [7] модель обнаружения аномалий объектов и сущностей в зоне анализируемого объекта КИИ в качестве прототипа, в которой вся получаемая информация преобразуется в многомерные временные ряды (МВР) с целью последующего интеллектуального анализа на основе машинного обучения, то для адаптации данной модели к образовательной организации требуется не только распознавание аномалий, идентифицируемых внутри технических систем, но и внедрение модуля распознавания эмоций субъектов и их действий. На основе корреляции видеопотока данных, снимаемого с помощью видеокамер контроля безопасности, и данных о физическом состоянии субъектов, снимаемых смарт-часами, интеллектуальная подсистема мониторинга принимает решение об аномальном поведении субъекта или группы субъектов.

Таким образом, каждая модель искусственного интеллекта распознает свой тип событий с целью выявления как технических, так и поведенческих аномалий, оценивает вероятности рисков нарушения безопасности каждого вида и передает сформированный массив данных в облачную подсистему комплексного интеллектуального анализа данных. Полученный массив данных анализируется и преобразуется в сценарий комплексной атаки, который сравнивается с множеством сценариев. Если коэффициент корреляции имеет значение выше порогового уровня, то принимается решение о реализации комплексного сценария контрмер.

С целью решения задачи идентификации и классификации аномалий различного типа, рассмотрим структуру и методику применения модели комплексного их обнаружения на объектах образовательной организации.

Модель комплексного обнаружения аномалий состояния зон объектов образовательной организации

Структурная схема предложенной системы обнаружения аномалий состояния зон объектов образовательной организации основана на синтезе методов анализа собираемых данных (рис. 1):

1. Метод выявления аномалий в технологических временных рядах (ТВР) на основе разности панорам в множестве выделенных окон наблюдения между реальными данными, полученными с сенсоров и данными, сгенерированными искусственной нейронной сетью (ИНС) [9]. Данный метод применим для технических объектов анализа и позволяет оценить для каждой аномалии вектор признаков, присущих ей.

76PSMN324
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

2. Метод выявления поведенческих аномалий на основе анализа моделью ИНС по распознаванию эмоций FER [10] данных, получаемых из видеоизображений и снятых с помощью смарт-часов, во взаимодействии с моделью IFO (Isolation Forest) [1], осуществляющей классификацию аномалий в действиях субъектов.

3. Для реализации модуля корреляции между аномалиями, когда один ансамбль нейронных сетей выявляет аномалии объектов, а другой ансамбль аномалии субъектов, предлагается рассмотреть использование метода совместного анализа данных на основе модели JADM (Joint Anomaly Detection Model) [12; 13].

В рамках предлагаемой модели ИПКМ ОС осуществляет обработку множества реальных данных в единицу времени $D^{(R)} = \left\{ d_1^{(R)}, d_2^{(R)}, ..., d_q^{(R)} \right\}, q = \overline{1,Q}$, поучаемых от множества сенсоров $S = \{sen_1, sen_2, ..., sen_i\}, i = \overline{1,I}$, множества видеокамер $Cam = \{cam_1, cam_2, ..., cam_j\}, j = \overline{1,J}$ и множества смарт-часов

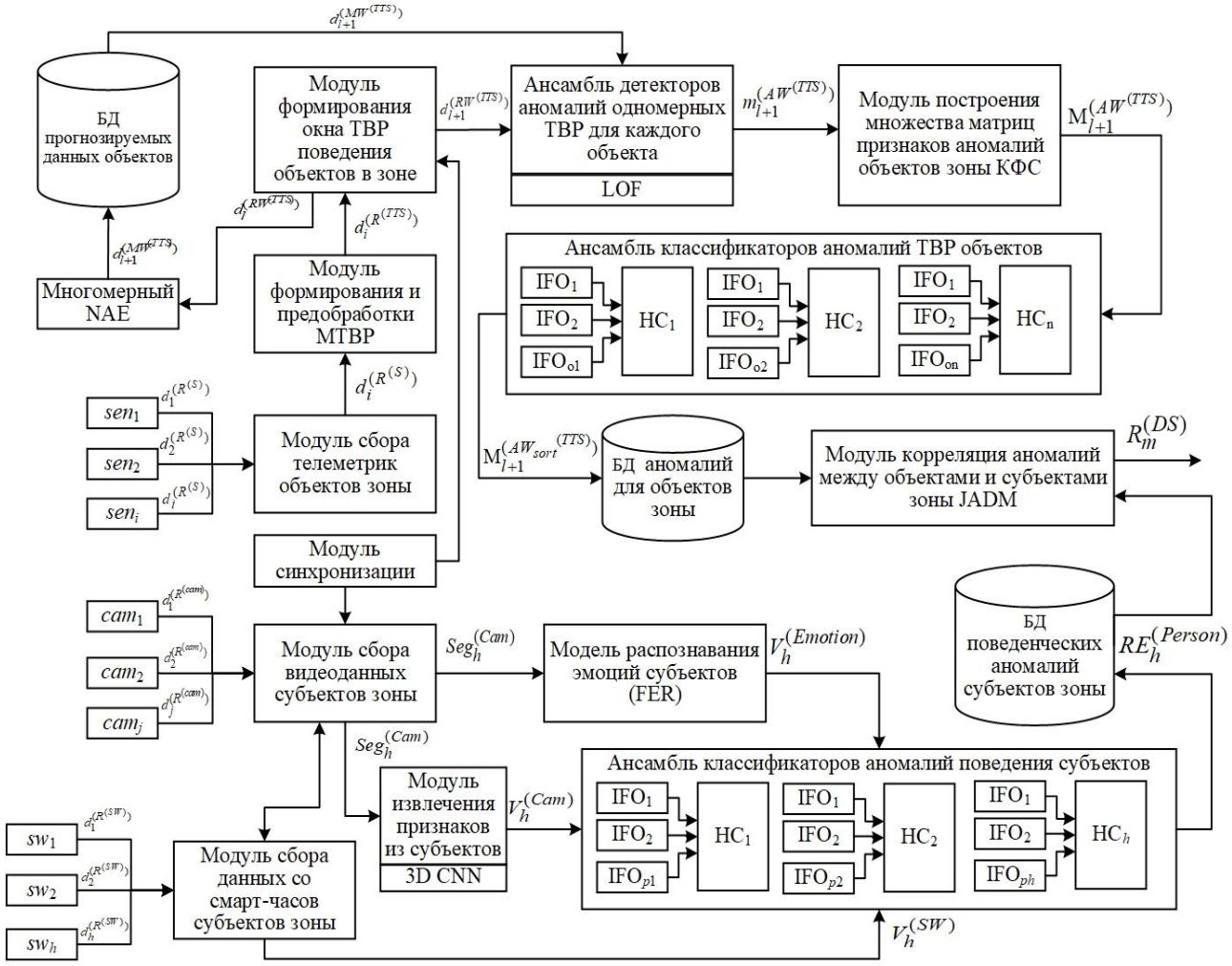

Рисунок 1. *Модель комплексного обнаружения аномалий состояния зон объектов образовательной организации (составлено автором)*

$SW = \{sw_1, sw_2, ..., sw_h\}, z = \overline{1,H}$ в множестве зон мониторинга $Z = \{z_1, z_2, ..., z_k\}, z = \overline{1,K}$, при этом для каждой зоны в дискретные моменты времени $T = \{t_1, t_2, ..., t_l\}, z = \overline{1,L}$ из множества C и S формируются постоянные подмножества $C = \{C_1, C_2, ..., C_y\}, y = \overline{1,Y}$,

76PSMN324
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

$S=\{S_1,S_2,...,S_w\}, w=\overline{1,W}$, а для множества $SW=\{SW_1,SW_2,...,SW_d\}, d=\overline{1,D}$ состав элементов подмножеств постоянно изменяется. С целью анализа сформированного в единицу времени массива данных $d_i^{(R)}$, получаемых с сенсоров, осуществляется его преобразование в многомерный телеметрический временной ряд (МТВР) $d_i^{(R^{(TTS)})}\left| d_i^{(R^{(TTS)})} \in D^{(R^{(TTS)})}\right.$ на основе фильтрации паразитных данных с последующей их нормализацией и разбиением данного ряда на множество дискретных окон $W=\{w_1,w_2,...,w_l\}, l=\overline{1,L}$.

С целью формирования множества параллельно моделируемых данных окон МТВР $D^{(MW^{(TTS)})}$ с помощью метода скользящего окна из временных рядов набора данных формируются обучающие и тестовые выборки, которые передаются в искусственную нейронную сеть, построенную на основе модели многомерного автоэнкодера NAE. Нейросетевой автоэнкодер NAE в задаче обнаружения аномалий предназначен для восстановления (реконструкции) фрагмента ТВР. Обнаружение аномалий осуществляется на основе порогового сравнения среднеквадратической (или абсолютной) ошибки между фактическими данными и восстановленным образом.

Данная модель после обучения на множестве $D^{(WR^{(TTS)})}$ позволяет прогнозировать поведение объектов до установленного момента времени на (*x*-*l*) — окон вперед:

$$D^{(MW^{(TTS)})}=\left\{\begin{matrix} d_1^{(MW^{(TTS)})}, d_2^{(MW^{(TTS)})},..., d_l^{(MW^{(TTS)})}, \\ d_{l+1}^{(MW^{(TTS)})}, d_{l+2}^{(MW^{(TTS)})},..., d_x^{(MW^{(TTS)})} \end{matrix}\right\}, x=\overline{1,X}. \quad (1)$$

Прогнозирование нормального поведения объектов необходимо для своевременного обнаружения множества аномалий $A=\{a_1,a_2,...,a_u\}, u=\overline{1,U}$. Каждая из аномалий представляет из себя отрезок временного ряда, имеющий набор отличительных признаков, который можно представить в виде вектора $\mathrm{p}_u^{(a_u)}\left|\mathrm{p}_u^{(a_u)}\in \mathrm{P}^{(A)}\right.$. С целью выявления аномалий NAE передает прогнозируемое моделируемое окно данных $d_{l+1}^{(MW^{(TTS)})}$ на ансамбль детекторов аномалий одномерных ТВР для каждого объекта. Данный модуль принимает с модуля формирования окна ТВР поведения объектов в зоне реальные данные окна $d_{l+1}^{(RW^{(TTS)})}$ и сравнивает с данными $d_{l+1}^{(MW^{(TTS)})}$, полученными от NAE, при этом формируется разность панорам.

С целью минимизации вероятности пропуска аномалии или ее ложного определения используют модель оценки выбросов с автоподстройкой порога (LOF — Local Outlier Factor) [14]. В отличие от статических моделей, которые используют фиксированный порог для определения выбросов, модель с автоподстройкой порога позволяет адаптировать порог θ на основе изменяющихся характеристик данных. В данной модели алгоритм автоматически рассчитывает порог, основываясь на статистических свойствах данных, таких как среднее значение, стандартное отклонение и разброс данных. При изменении статистических характеристик данных, например, при появлении новых выбросов или изменении распределения данных, модель автоматически пересчитывает порог, чтобы учитывать данные

76PSMN324
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

изменения в будущем. Такой подход позволяет более эффективно и точно обнаруживать выбросы в данных, снижая вероятность ложных срабатываний и улучшая общую производительность модели оценки выбросов. Таким образом, на выходе одномерных LOF-детекторов формируются подмножество точек, которые превышают для каждого показателя в окне соответствующий порог θ, образуя матрицу возможных аномалий окна w_{l+1} объекта *n*.

Однако LOF-детекторы выступают в роли предобрабатывающих модулей: для точной идентификации аномалии, получения соответствующего вектора признаков и решения задачи кластеризации целесообразно использование модели обнаружения аномалий на основе изолирующего леса (IFO — Isolation Forest).

Суть работы модели IFO заключается в том, что она создает лес деревьев решений, где каждое дерево строится на основе случайного признака и случайного разделения данных. Алгоритм IFO предполагает, что аномалии в данных имеют меньшее количество разделений по сравнению с нормальными образцами. При обучении модели каждое дерево строится путем случайного выбора признака и случайного выбора значения для разделения данных. Аномалии обычно будут находиться ближе к корню дерева из-за их более короткого пути, в то время как нормальные образцы будут иметь более длинный путь к листьям. После построения леса деревьев модель может определить, какие образцы являются аномалиями, и какие — нормальными. Данная модель обладает высокой эффективностью и быстродействием, особенно когда имеется большое количество признаков в данных.

Оценка качества методов обнаружения аномалий в временных рядах параметров производится с помощью традиционных метрик качества классификации и TaPR — метрики оценки обнаружения аномалии и корректности границ аномалии в ТВР. С целью количественной оценки используются классические метрики: коэффициент точности, коэффициент полноты, F-мера.

Таким образом полученное на входе множество матриц $\mathrm{M}_{l+1}^{(AW^{(TTS)})}$ точек возможных аномалий для каждого объекта, находящего в зоне мониторинга формируется множество матриц аномалий $\mathrm{M}_{l+1}^{(AW_{sort}{}^{(TTS)})}$ на выходе с ансамбля классификаторов ТВР объектов, которые записываются в базу данных аномалий объектов, находящихся в момент времени t_{l+1} в зоне мониторинга.

Параллельно данному процессу на основе использования модуля синхронизации осуществляется процесс идентификации и классификации поведенческих аномалий субъектов, находящихся в момент времени t_{l+1} в зоне мониторинга z_k. Для этого подмножество сегментов видеоданных $D_h^{(R^{(C)})}$, получаемых от подмножества видеокамер, находящихся в зоне мониторинга z_k, с момента времени t_l до момента времени t_{l+1} поступают в модуль сбора видеоданных субъектов зоны на основе подмножества сообщений *M*, передаваемого от подмножества смарт-часов SW_d, с которыми установлено соединение. Полученные отрезки передаются на модуль распознавания эмоций FER для каждого субъекта в зоне мониторинга, который определяет эмоциональное состояние субъекта в виде вектора $V_h^{(Emotion)}$. В качестве аномальных эмоций выбираются грусть и злость.

76PSMN324
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

При этом, для определения нетипичного положения частей тела, наличия холодного или огнестрельного оружия и несанкционированных действий субъектов, а также их психологического и физического состояния в текущих условиях в момент времени t_{l+1}, данные с подмножества смарт-часов (например, пульс субъекта) и данные видеоотрезков с модуля сбора видеоданных субъектов зоны, а также оценка эмоционального состояния субъекта $V_h^{(Emotion)}$ поступают на подмножество IFO-детекторов. IFO-детекторы позволяют определить аномальные действия субъектов (как легитимных, так и посторонних) и с помощью HC_h нейронной сети (персональный ассистент субъекта) классифицировать поведенческие аномалии. Каждый сегмент видео между моментом времени t_l и t_{l+1} содержит несколько клипов по 64 кадра и для каждого 64 кадра извлекаются признаки, формируемые в вектор $V_h^{(Cam)}$ (рис. 2).

Моделирование долгосрочной временной зависимости между векторами $V_h^{(Cam)}$ в видеопоследовательности выполняется рекуррентной нейронной сетью (RNN) и моделью временного внимания первого уровня. На этом этапе извлеченные визуальные особенности передаются в RNN, в частности в LSTM, для моделирования временной эволюции аномалий в видео. Временное внимание первого уровня обеспечивает различительные веса внимания для временных сегментов с вероятным возникновением аномалий.

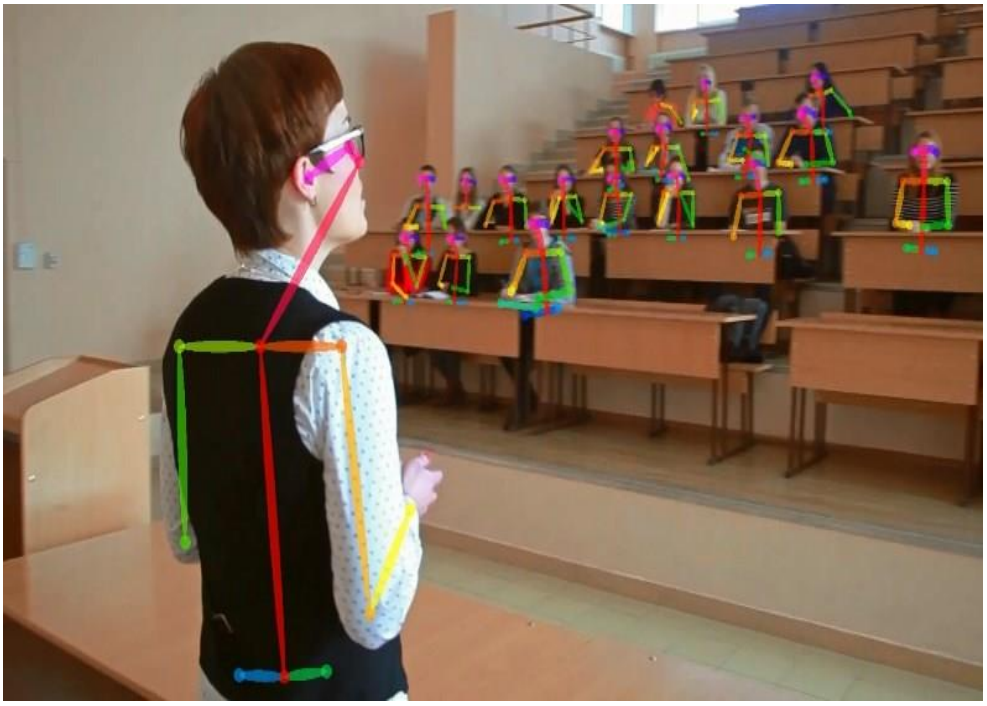

Рисунок 2. *Визуальное представление вектора признаков* $V_h^{(Cam)}$ *[12]*

Чтобы получить временную связь между сегментами видео, используется LSTM «многие ко многим». Хотя временное моделирование видеосегментов достигается с помощью LSTM, некоторая визуальная информация теряется в данном процессе из-за активированных сигмовидных ворот обучения в LSTM. Поэтому, чтобы сохранить свойства пространственно-временной карты объектов, целесообразно использовать сверточную нейронную сеть CNN. Поэтому на втором уровне внимания благодаря использованию CNN осуществляется

агрегирование множества векторов $V_h^{(Cam)}$ с целью определения устойчивого поведенческого состояния субъекта.

Обучение множества персональных ассистентов целесообразно производить на основе совокупности нормальных и аномальных данных, например, на начальном этапе обучающей выборкой может выступать UCF-Crime [15] (одиночные атаки или их комбинации с целью реализации комплексной атаки).

Полученное множество поведенческих аномалий $RE_h^{(Person)}$ сохраняются в базе данных для последующего дообучения персональных ассистентов и передаются в модуль корреляция аномалий между объектами и субъектами зоны, функционирующий на основе модели JADM. Так как важна последовательность взаимодействия субъектов и объектов целесообразно для обучения данной модели использовать ансамбль нейросетевых автоэнкодеров (NAE) с долгой-краткосрочной памятью (LSTM), на выходе которой будет получен вектор оценки риска нарушения комплексной безопасности $R_m^{(DS)}$ в зоне объекта контроля z_k.

Выводы

При анализе и управлении рисками специфика образовательной организации создает дополнительные сложности технического, психологического и информационного характера, что говорит о необходимости реализации интеллектуальных методов, которые будут эффективны, несмотря на невысокую формализованность объекта исследования с точки зрения моделирования сценариев атак.

Предлагаемая модель комплексного обнаружения аномалий состояния зон объектов образовательной организации осуществляется на основе внедрения дополнительных сенсоров и смарт-часов, осуществляющих непрерывную передачу данных о поведении как объектов, так и субъектов контроля, тем самым позволяя анализировать моделями искусственного интеллекта (персональными ассистентами субъектов и «цифровыми двойниками» объектов) состояние защищенности зоны мониторинга и оценивать комплексный риск нарушения ее безопасности. С целью. повышения точности распознавания поведенческих аномалий субъектов предлагается использовать модели распознавания эмоций FER на основе сверточных нейронных сетей и детекторов на основе изолирующего леса IFO.

ЛИТЕРАТУРА

1. 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. — EDN PJZWIF.
2. 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. — EDN TSXAOF.

3. 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. — EDN IACHEN.

4. Зубарев, Н.Ю. Анализ факторов, влияющих на реализацию инноваций в научно-технических разработках университета / Н.Ю. Зубарев // Вестник евразийской науки. — 2022. — Т. 14, № 6. — EDN DMIXFB.

5. 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. — EDN WFABOH.

6. 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. — EDN UBVLTK.

7. Перекопновский, Д.И. Применение компьютерного зрения и искусственного интеллекта в современном мире / Д.И. Перекопновский // Фундаментальные и прикладные научные исследования: актуальные вопросы современной науки, достижения и инновации: Сборник научных статей по материалам XIII Международной научно-практической конференции, Уфа, 15 декабря 2023 года. — Уфа: Общество с ограниченной ответственностью "Научно-издательский центр "Вестник науки", 2023. — С. 262–265. — EDN UAUDNM.

8. 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. — EDN FJPFKC.

9. Васильев, В.И. Обеспечение информационной безопасности киберфизических объектов на основе прогнозирования и обнаружения аномалий их состояния / В.И. Васильев, А.М. Вульфин, В.Е. Гвоздев [и др.] // Системы управления, связи и безопасности. — 2021. — № 6. — С. 90–119. — DOI 10.24412/2410-9916-2021-6-90-119. — EDN TDDYFH.

10. Рюмина Е.В., Карпов А.А. Аналитический обзор методов распознавания эмоций по выражениям лица человека // 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. 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. — EDN WKOUDJ.

12. 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. — EDN KERSAW.

13. 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. — EDN IKAOTB.

14. Breunig, Markus & Kröger, Peer & Ng, Raymond & Sander, Joerg. (2000). LOF: Identifying Density-Based Local Outliers. ACM Sigmod Record. 29. 93–104. 10.1145/342009.335388.

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. — EDN RISLVB.

Soskovets Albert Vladimirovich
Omsk State Technical University, Omsk, Russia
E-mail: soskovets.albert@mail.ru
ORCID: https://orcid.org/0009-0003-2542-2592

Milczarek Tadeusz Petrovich
Omsk State Technical University, Omsk, Russia

Ensuring comprehensive security of an educational organization based on intelligent monitoring

Abstract. The study substantiates the need to implement an intelligent complex monitoring subsystem at the facilities of educational organizations, which allows assessing the complex risk of a violation of its security. An implementation of this subsystem is proposed based on the use of an ensemble of artificial intelligence models that detects anomalous behavior of both objects and subjects in the observation area. The novelty of the proposed model is that to improve the accuracy of recognizing behavioral anomalies of subjects, FER emotion recognition models based on convolutional neural networks and models for analyzing personal health characteristics of subjects based on their reading of data from smart watches are used. The combination of these models forms many personal assistants. To improve the accuracy of complex risk assessment, JADM anomaly correlation models are used.

Keywords: intelligent monitoring; anomaly detectors; FER emotion recognition models; neural network autoencoder with long short-term memory; personal assistant; CNN