**DOI 10.36622/VSTU.2023.4.26.002**
**УДК 004.056**

# ЦЕЛЕПОЛАГАНИЕ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ ПО СОЗДАНИЮ ИНСТРУМЕНТАРИЯ АВТОМАТИЗАЦИИ ВЫЯВЛЕНИЯ И РЕГУЛИРОВАНИЯ РИСКОВ ДЕВИАНТНОГО ПОВЕДЕНИЯ СОТРУДНИКОВ КОРПОРАЦИЙ

**А.Г. Остапенко, А.Г. Зимницкий, Е.А. Москалева**

На основе всестороннего исследования предметной области обоснована актуальность создания инструментария выявления и регулирования рисков девиантного поведения сотрудников корпорации в контексте обеспечения их безопасности. Рассмотрение аналогов позволило осуществить целеполагание проектной деятельности по линейке взаимно однозначного соответствия выявленных противоречий, поставленных задач, ожидаемых результатов, их новизны, практической ценности и теоретической значимости. В соответствии с вышеизложенным предлагается архитектура создаваемого инструментария, включающая разнообразные библиотеки и модули, осуществляется демонстрация их использования на практических примерах автоматизированного анализа мимических эмоций (злость, отвращение, страх, радость, грусть, удивление и др.) человека.

Ключевые слова: риск, девиантное поведение, корпорация, целеполагание, эмоции.

## Введение

Эмоциональная нестабильность, напряжённость, преобладание низкого самоконтроля присуще субъектам склонным к девиантному поведению.

В основе большинства правонарушений лежат следующие эмоции: страх и гнев, которые приводят к немедленной реакции субъекта. Исходя из общей теории напряжения (ОТН) в криминологии, можно сделать вывод, что преступления являются результатом высокого эмоционального напряжения субъекта, приводящего к выплеску негативных эмоций [1]. Вместе с тем, видеоинформация об эмоциональном состоянии субъекта позволит с высокой точностью судить об актуальных и важных для него в определённый момент времени вещах.

В настоящее время видеоконтроль активно внедряется в корпорациях и уже нет смысла в использовании одной только базовой системы видеонаблюдения, поэтому она наполняется дополнительными модулями для обнаружения и анализа различных событий безопасности, что, в свою очередь, позволяет не только фиксировать происходящее в режиме реального времени, но и предоставляет возможность для предварительного анализа состояний и событий для принятия мер по предотвращению угроз. Кроме того, в современных системах видеонаблюдения существует запрос на создание подсистем, способных анализировать состояние субъекта, чему может способствовать совокупность его жестов и мимики, применяемых в процессе невербального общения. Мимика является отображением внутреннего эмоционального состояния посредством динамики лицевых мышц, обработав которую можно осуществить оценку риска совершения девиантного поведения субъектом.

Говоря об обеспечении корпоративной безопасности в данной сфере, можно увидеть возрастающую актуальность данного вопроса по причине высокого количества инцидентов на рабочих местах, предупреждение и пресечение которых весьма актуальны в работе с персоналом. Поэтому сейчас широко распространено использование модулей систем видеонаблюдения на основе компьютерного зрения: распознавание лиц, распознавание поз, детектирование опасных объектов и оружия, детектирование оставленных вещей в зонах общественного использования, распознавание гос. номеров автотранспорта.

В связи с увеличением террористической активности и ростом количества других инцидентов на территории предприятий возрастает потребность в анализе поведения субъекта с целью профилактики инцидентов и утечки чувствительных данных. Распознавание эмоций в совокупности с другими признаками (распознавание нетрезвого состояния, опасных предметов, оружия) в текущий момент времени позволит осуществить оценку риска возникновения девиантного поведения и правонарушения, в дополнении с интернет-профилем сотрудника можно оценить – является ли его действие продуктом состояния аффекта или же за этим стоит глубинные аномалии.

**Аналоги**

1. MorphCast – иностранный фреймворк для распознавания лицевых мышц и, соответственно, эмоций. Имеет ограниченную бесплатную версию, платная имеет стоимость от 300 евро в месяц. Предоставляет API для взаимодействия, нет возможности развернуть On-Premise решение, что может быть не применимо для использования на территории предприятия [2].

2. ITV “Face-Интеллект” – российское ПО для распознавания лиц, обладает высокой скоростью работы, может применяться для автоматического учёта рабочего времени, отсутствует анализ эмоций субъекта [3].

3. FaceReader – иностранное проприетарное решение типа Software-as-a-Service, предоставляет решение под клиента для распознавания эмоций. Находится на серверах Microsoft Azure, что также не во всех случаях может быть приемлемо для конечного пользователя данного сервиса [4].

4. Allcontrol – инструмент, обладающий широким функционалом в сфере обеспечения физической безопасности: защита периметра (выявление инцидентов на территории корпорации), распознавание лиц, нахождение данных о субъекте с использованием OSINT, отсутствует возможность отображения детальных рекомендаций для ЛПР с целью коррекции матрицы доступа [5].

**Целеполагание**

Объект исследования представляет собой эмоциональное состояния работника в контексте обеспечения информационной безопасности предприятия.

Предметом исследования является оценка риска девиантного поведения по совокупности психоэмоциональных характеристик работника.

Целью данной работы является программная реализация инструментария, предоставляющего функционал анализа психоэмоционального состояния субъекта в режиме реального времени, выдачи интеллектуальных подсказок для ЛПР и сопоставления данных пользователя с его профилем в социальных сетях для составления эмоционального портрета субъекта с последующей оценкой и регуляцией рисков корпорации, в целях обеспечения её безопасности.

Опираясь на вышеизложенное, представляется возможным выделить следующие противоречия между:

1. Необходимостью анализа психофизических компонентов личности с дальнейшей оценкой риска и отсутствием отечественных инструментов для решения данной задачи.

2. Необходимостью создания базы знаний подсказок для ЛПР и пользователей и отсутствием набора данных для её разработки.

3. Стандартной совокупностью психоэмоциональных компонентов, оценивающих субъекта в краткосрочной перспективе и отсутствием дополнительного учёта также интернет-профиля субъекта, что позволит проанализировать, является ли проявление девиантного поведения эпизодическим или имеет системный характер за счёт сформированных и проявившихся в социальных сетях его убеждений.

Исходя из поставленных противоречий и цели работы можно выделить следующие задачи исследования.

1. Создание программно-технический комплекса, на основе оборудованного видеокамерой рабочего места внутреннего пользователя корпоративной сети, обеспечивающего в реальном времени

возможность анализировать (по мышцам лица) психофизическое состояние каждого пользователя и оценивать риски его девиантного поведения, нарушающего безопасность функционирования сети.

2. Разработка программного блока (возможно, на основе нейросети), позволяющего администрировать доступ пользователем с учётом показателей их персональных рисков, включая возможность подсказок самим пользователем по улучшению своего психоэмоционального состояния (в целях повышения производительности и безопасности производственного процесса), а также статистический анализ, способный обеспечить оптимизацию использования кадрового потенциала (с учётом его текущего состояния) и повышение эффективности реализации корпоративных проектов.

3. Дополнение вышеуказанных персональных данных анализом сетевой активности пользователей в социо-информационном пространстве (зеркале информационно-психологического состояния пользователя в соц. сетях и пр.), где риск-оценка поможет уберечь работника от необдуманных социальных реакций, а соответствующая профилактическая работа кадровых служб способна оградить его от участия в промышленном шпионаже и других противоправных действиях (нужно только отделить сиюминутные эмоции от глубоких убеждений, направленных против корпорации и государства), с использованием нейросетевых технологий.

Планируемые результаты проекта:

1. Методика оценки риска на основе психоэмоциональных компонентов и разработанный инструмент риск-анализа девиантного поведения;

2. Программный модуль администрирования доступа пользователей на основе их персональных показателей, выдачи подсказок для конечных пользователей и статистический анализ психоэмоциональных данных;

3. Программный модуль, производящий оценку риска на основе совокупности психоэмоциональных компонентов, полученных в определённый момент времени, и данных о сетевой активности пользователя в социо-информационном пространстве.

В отличии от аналогов ожидается следующая новизна результатов:

1. При разработке программного обеспечения использовался новый метод распознавания девиатного поведения человека, который основывается на общей теории напряжения, что позволило произвести прогноз деструктивного действия человеком до его совершения с определенной вероятностью.

2. Предусмотрена возможность психоэмоциональной коррекции поведения конкретных пользователей корпорации.

3. Совместный анализ психофизического состояния и данных сетевой активности пользователей в социо-информационном пространстве даст объективный портрет, значимый для обеспечения информационной безопасности корпорации в рамках компетенций отдельно взятого пользователя.

Практическая ценность результатов видится в следующем:

1. Создаваемый инструментарий риск-анализа может быть интегрирован в системы видеонаблюдения корпораций, что, в свою очередь, увеличит эффективность обеспечения информационной безопасности.

2. Разрабатываемый модуль позволит регулировать доступ к корпоративным ресурсам на основе анализа персональных показателей пользователя, что способствует предотвращению несанкционированного доступа и потенциальных утечек информации. Статистический анализ психоэмоциональных данных дает возможность руководству корпорации анализировать общее эмоциональное состояние персонала, определять субъектов с потенциальным риском девиантного поведения.

3. Дополнение данных о психоэмоциональных компонентах сведениями об активности пользователя в социо-информационном пространстве позволит проактивно реагировать на потенциальные угрозы, связанные с девиантным поведением сотрудников. Анализ совокупности этих данных позволит выявить не только мгновенные изменения в поведении, но и более глубокие, скрытые.

Теоретическая значимость результатов видится в следующем:

1. Разрабатываемые методики риск-оценки девиантного поведения на основе психоэмоциональных компонентов позволит выявить взаимосвязь между невербальными сигналами и внутренним психоэмоциональным состоянием человека, что облегчит задачу распознавания и предотвращения девиантного поведения;

2. Анализ зависимости между изменениями в психоэмоциональном состоянии субъекта и его эффективностью позволит прийти к созданию новой методики прогнозирования внутренних угроз в корпорации, которая может быть использована для формирования политик безопасности;

3. Обнаружение корреляции между определёнными шаблонами поведения в социо-информационном пространстве и поведенческими рисками на рабочем месте может способствовать разработке теоретических моделей для прогнозирования и предотвращения инсайдерских угроз.

**Актуальность**

В настоящее время увеличивается количество инцидентов на рабочих местах в результате девиантного поведения сотрудников, то есть их поведения, отличающегося от социально одобряемого и выражающегося в единичном или системном нарушении общепринятых и корпоративных норм. В целом, девиантное поведение — это проблемное поведение, имеющее свойства устойчивости, длительности и повторяемости.

Сегодня оно может быть спровоцировано деструктивным интернет-контентом, реализующим неконтролируемое и целенаправленное воздействие через размещение провокационной или запрещенной информации, что может вызвать деструктивные изменения в личностных чертах и качествах, которые способствуют возникновению девиантного поведения. Это также подчеркивает высокую потребность в изучении и создании механизмов, способных выявлять и прогнозировать опасное для корпорации поведение и давать рекомендации лицам, принимающим решение (ЛПР), по снижению деструктивного человеческого фактора на корпоративные процессы, связанные с обеспечением информационной безопасности, адекватным и своевременным реагированием на угрозы.

В контексте корпоративной безопасности такое поведение может включать в себя акты, создающие угрозу информационной безопасности, такие как несанкционированный доступ, кража данных, межличностные конфликты, и т.д.

Многочисленные исследования подтверждают связь между эмоциональными состояниями и поведенческими реакциями человека, в том числе и влияние стресса на принятие решений и самоконтроль. При этом эмоции могут мощно, предсказуемо и всепроникающе влиять на процесс принятия решений.

Для глубокого изучения влияния эмоций на вероятность девиантного поведения необходимо обратиться к общей теории напряжения из криминологии, которая утверждает, что преступления являются результатом эмоционального напряжения в жизни человека, которое приводит к негативным эмоциям, таким как печаль, тревога или гнев [1]. Очевидно, что гнев и страх, вызванные напряжением, особенно способствуют преступному поведению, в наибольшей степени порождают девиантное поведение и применение неправомерных методов борьбы с проблемами.

Об этом свидетельствуют нижеприведенная классификация [6]:

1. Влияние гнева на совершение правонарушения:

1.1. Мотивация к агрессивным действиям. Гнев часто является мотивирующим фактором для агрессивного или насильственного поведения. В состоянии гнева человек может чувствовать себя оправданным в своих действиях, в том числе в применении насилия.

1.2. Снижение контроля. Гнев может уменьшить самоконтроль и увеличить импульсивность, что приводит к менее осмысленным и более рискованным действиям, включая совершение преступлений.

1.3. Влияние на восприятие ситуации. Гнев может исказить восприятие ситуации, заставляя человека видеть больше угроз или враждебности в окружающей среде, что может привести к агрессивному ответу.

2. Влияние страха на совершение правонарушения:

2.1. Сдерживающий фактор. Страх перед последствиями может быть сдерживающим фактором, предотвращающим совершение преступлений. Это особенно верно, когда человек воспринимает высокую вероятность быть пойманным или наказанным.

2.2. Мотивация для отчаянных действий. В некоторых случаях страх может также мотивировать на совершение преступлений, особенно если человек чувствует, что находится под угрозой. Например, страх перед физическим насилием может побудить к преступным действиям.

2.3. В зависимости от обстоятельств, страх может влиять на процесс принятия решений, заставляя человека выбирать более безопасные или менее рискованные варианты поведения.

Отсюда следует вывод о том, что эмоции, которые с наибольшей вероятностью может привести к насилию — это страх и гнев, которые имеют отрицательную гедонистическую ценность, негативно оцениваются и имеют немедленный характер. То есть, в контексте принятия решений, страх и гнев представляют собой немедленные реакции на событие, ситуацию, человека.

Гнев и страх возникают, когда субъект воспринимает угрозу своей безопасности. Страх описывается как эмоциональный ответ, отталкивающий человека от того, что он переживает или ожидает пережить, будь то реальное или воображаемое. В то время как страх заставляет субъекта чувствовать себя уязвимым, гнев может давать и усиливать энергию, то есть, гнев может стать реакцией на переживания страха [7]. Глубоко деструктивные действия являются реакцией на страх и обиды [8]. Необходимо осознавать, что анализ, основанный исключительно на эмоции страха, может привести к ошибочным результатам из-за её способности к накоплению и последующему превращению в гнев. Часто перед тем, как совершить деструктивные действия, преступник испытывает страх, однако доминирующей эмоцией обычно является гнев, поэтому крайне важно иметь оценки эмоционального состояния исследуемой личности. Одно из исследований отмечает, что эмоции связаны между собой, так что, например, страх может вызвать гнев [9]. Это происходит потому, что при оценке ситуации, когда человек осознает, что его страх вызван действиями другого человека, возникает гнев по отношению к этому человеку за то, что он создал угрозу личному благополучию.

Экман и Фризен (1978) разработали систему FACS (Facial Action Coding System), которая классифицирует движения мышц лица и соотносит их с конкретными эмоциями. Система FACS стала основой для многих исследований в области распознавания эмоций, и ее применение в контексте обеспечения информационной безопасности может дать новые возможности для прогнозирования девиантного поведения. Система кодирования мышц лица представляет собой анатомический метод, предназначенный для категоризации всех заметных движений лица, основывающийся на работе лицевых мышц. Этот подход включает разбиение выражений лица на базовые составляющие, известные как единицы действия (Action Units).

Эмоциональные выражения, такие как злость, обычно проявляются в определенных сочетаниях единиц действия (AU), например, в форме паттернов

$$AU4 + AU5 + AU7 + AU24.$$

Каждая мышца лица ассоциируется с конкретной единицей действия, что позволяет точно анализировать выражения эмоций на лице.

Не все лицевые мышцы поддаются одинаковой степени контроля, и движения некоторых из них являются более надежными индикаторами эмоций, чем другие. Это связано с тем, что многие мышцы лица не полностью контролируются волей человека. В результате, имитировать или подделать некоторые эмоциональные выражения бывает сложно, так как они требуют

активации специфических мышц, которые не всегда поддаются сознательному контролю. Исследование показало, что всего 10% участников могли добровольно опускать уголки рта без движения подбородком [11]. Тем не менее, те же мышцы, которые трудно контролировать осознанно, активировались автоматически, когда люди на самом деле испытывали соответствующие эмоции, вызывающие такие движения. Это подчеркивает, что некоторые мышцы лица реагируют преимущественно на подлинные эмоциональные переживания, а не на сознательные попытки их имитации.

Возможно, человек попытается сокрыть свои чувства, например, прикрыть их улыбкой. Однако, при этом не устраняются признаки эмоций в движениях лба и век. Можно попытаться компенсировать движения одних лицевых мышц, напрягая другие, которые производят обратное действие, чтобы в итоге выражение лица осталось неизменным. Например, радостную улыбку можно скрыть, сжимая губы и поднимая подбородок. Однако такое противодействующее движение мышц может само по себе выдавать обман. Это связано с тем, что одновременная активация как контролируемых, так и неконтролируемых мышц может придать лицу неестественный, напряженный вид.

Для распознавания эмоций сегодня используются следующие инструменты:

1. Распознавание эмоций на основе выражений лица (FACS) [10].

2. Распознавание эмоций на основе аудиального контента. Данное решение реализуется через анализ изменения тона и энергии человеческого голоса. Отдельно на одних и тех же людях проводились эксперименты по распознаванию эмоций из заданного набора аудио и видеозаписей. По сравнению с подходом, основанным на визуальном выражении лица, методы, основанные на аудио, такие как методы автоматического распознавания речи, не были эффективными в классификации печали, которая была ошибочно классифицирована как нейтральная, и наоборот [12].

Методы для решения указанных задач подразделяются на нейросетевые и на не использующие нейросети.

Нейросетевые методы:

1. Сверточные нейронные сети (CNN): Способны обрабатывать входящее изображение, определять значимость разных деталей на изображении и различать их друг от друга. Они автоматически и эффективно извлекают признаки из изображений, что делает их особенно полезными для анализа мимики.

2. Рекуррентные нейронные сети (RNN): Эти сети используются для обработки последовательностей данных, например, речи, что делает их подходящими для распознавания эмоций на основе аудио. Они могут учитывать контекст и изменения в тональности голоса, что важно для понимания эмоций.

Методы, не использующие нейросети:

1. Support Vector Machine (SVM): Этот метод используется для классификации и регрессионного анализа. SVM может быть применен для определения эмоций, классифицируя данные лица или речи на основе обученных моделей.

2. K-Nearest Neighbors (KNN): Этот метод классификации основан на изучении сходств между различными точками данных. KNN может использоваться для распознавания эмоций, сравнивая новые данные с уже классифицированными образцами.

3. Histogram of Oriented Gradients (HOG): Этот метод используется для извлечения признаков из изображений, особенно полезен для распознавания эмоций в мимике, анализируя формы и ориентацию градиентов на изображениях лица.

Таков ландшафт предметной области, которой посвящается настоящая работа:

- необычные эмоциональные всплески. Анализ эмоциональных компонентов (в частности, страха и гнева) позволит дать информацию о вероятности совершения девиантного поступка.

- наличие состояние алкогольного или наркотического опьянения у субъекта коррелирует с повышенным риском проявления девиантного поведения.

- детектирование предметов, представляющих опасность для людей и окружающей среды (оружие и т.д.).

Учитывая изложенное выше, полноценная система выявления девиантного поведения должна базироваться на компонентах, со следующим функционалом:

1. Анализ психоэмоционального состояния позволит выявить критические моменты, когда субъект наиболее склонен к девиантному поведению и совершению противоправного действия.

2. Обнаружение на видеокадре систематически опасных субъектов с целью предотвращения инцидентов, представляющие угрозу для общества и корпорации;

3. Распознавание субъектов, временно находящихся в неадекватном состоянии, также позволит предупредить нарушение корпоративной безопасности.

**Архитектура создаваемого инструментария**

Одной из задач данной работы являлась программная реализация решения по анализу эмоций пользователя в режиме реального времени на языке программирования Python, в котором были использованы следующие библиотеки:

1. Flask – веб-фреймворк Python, используемый для создания веб-приложений. Является легким и модульным, что делает его хорошим выбором для простых веб-приложений и микросервисов. В данном решении используется для создания веб-интерфейса приложения;

2. Altair – библиотека визуализации данных для Python. Она основана на Vega и Vega-Lite, что позволяет создавать сложные интерактивные визуализации с помощью простого синтаксиса;

3. OpenCV (cv2) – мощная библиотека для обработки изображений и видео, широко используется в приложениях компьютерного зрения, таких как распознавание лиц, анализ движения и многие другие;

4. Dlib – библиотека машинного обучения, содержащая различные инструменты для выполнения простых и сложных задач машинного обучения. В данном ПТК она используется для распознавания лиц и ключевых точек на лице;

5. TensorFlow (Keras) – популярная библиотека для машинного обучения и глубокого обучения, разработанная Google. Keras является высокоуровневым интерфейсом для TensorFlow, предназначенным для быстрого создания и обучения нейронных сетей;

6. Pandas – библиотека для анализа и обработки данных, которая предоставляет удобные структуры данных и операции для манипулирования числовыми таблицами и временными рядами;

7. NumPy – библиотека, поддерживающая многомерные массивы и матрицы, вместе с большим набором функций для работы с этими массивами. Широко используется в научных и инженерных приложениях;

8. SciPy – библиотека, используемая для научных и технических вычислений. В этом проекте используется для операций с изображениями и других вычислений;

9. Imutils – набор удобных функций для упрощения базовых операций с изображениями в OpenCV, таких как вращение, изменение размера, отображение.

Для распознавания эмоций используются нейросетевая модель XCeption – это модель глубокого обучения, разработанная Франсуа Шолле в Google [13]. Она представляет собой расширение и улучшение архитектуры Inception, основанной на CNN и известной своей эффективностью в распознавании изображений. Отличительной особенностью Xception является использование модулей глубокой свертки, которые разделяют каналы входных данных и обрабатывают их отдельно перед их последующим смешиванием. Это повышает эффективность и точность модели. Xception обеспечивает более эффективное использование вычислительных ресурсов по сравнению с традиционными CNN, благодаря своей уникальной архитектуре. Данная модель была обучена на данных FER-2013 (Facial Emotion Recognition dataset) и имеет общую точность предсказания 64.5% [14].

Процесс распознавания эмоций в данном проекте выглядит следующим образом:

1. Захват видеопотока. На этом этапе используется библиотека OpenCV для захвата видеопотока через веб-камеру.

2. Обнаружение лиц и ключевых точек. Dlib используется для обнаружения лиц и ключевых точек на каждом кадре видеопотока, используя гистограмму ориентированных градиентов.

3. Изменение разрешения лица до 48x48 пикселей.

4. Предсказание эмоций, основываясь на предобученной модели XCeption, которая извлекает признаки из изображений лиц, такие как форма губ, глаз, бровей и их положение, которые являются ключевыми индикаторами эмоционального состояния.

Создаваемый программно-технический комплекс состоит из следующих компонентов:

1. Главная страница (index) – содержит информацию о модуле и его функционале (рис. 1).

2. Вступительная страница (video) – страница для начала видеозаписи пользователем (рис. 2).

3. Страница обработки видеоданных (video_1) – содержит информацию о результатах распознавания эмоций в режиме реального времени (рис. 3).

4. Панель результатов распознавания эмоций пользователя (video_dash) содержит информацию об анализе эмоций одного пользователя и о глобальной статистике (рис. 4-6).

Все приведенные на рис. 1-6 компоненты цветные. На рис. 6 показаны выводимые кривые эмоций с расшифровкой цветов, обозначающих ту или иную эмоцию, поэтому график наглядный. Для более понятного вида иллюстрации при черно-белой печати на рис. 8 полученные кривые дополнительно пронумерованы.

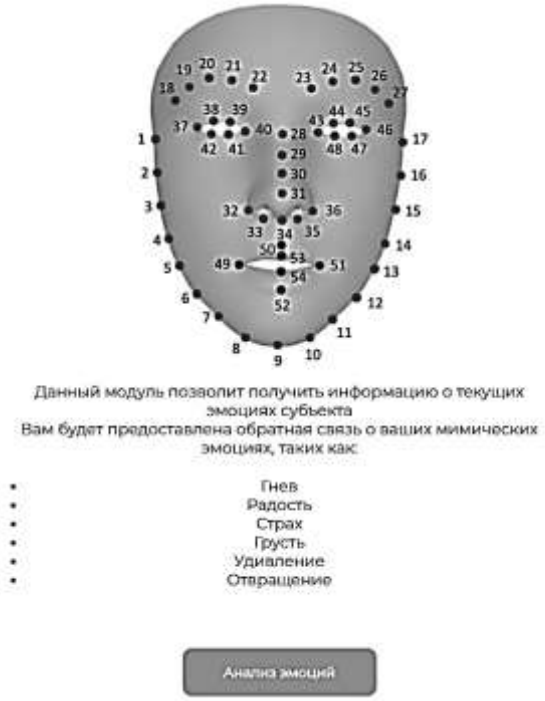


Рис. 1. Стартовая страница

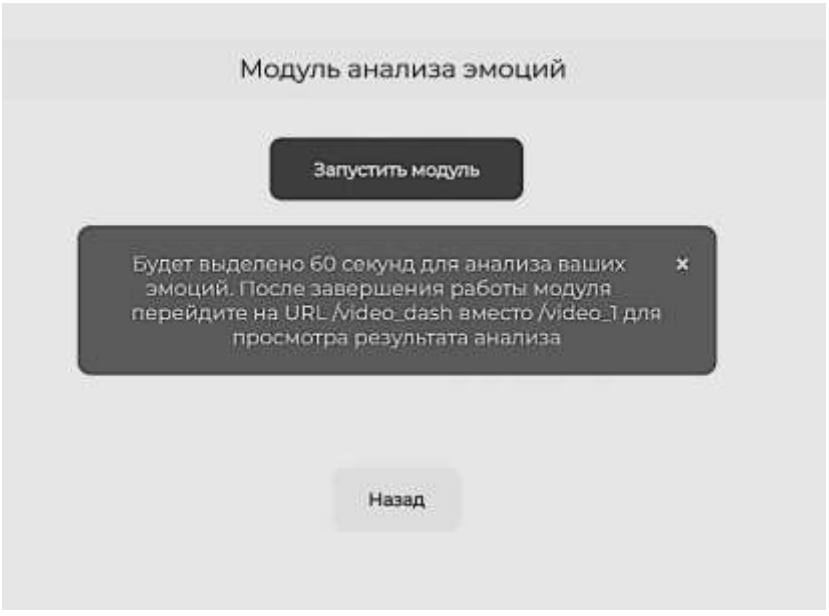


Рис. 2. Вступительная страница


Рис. 3. Страница обработки видеоданных

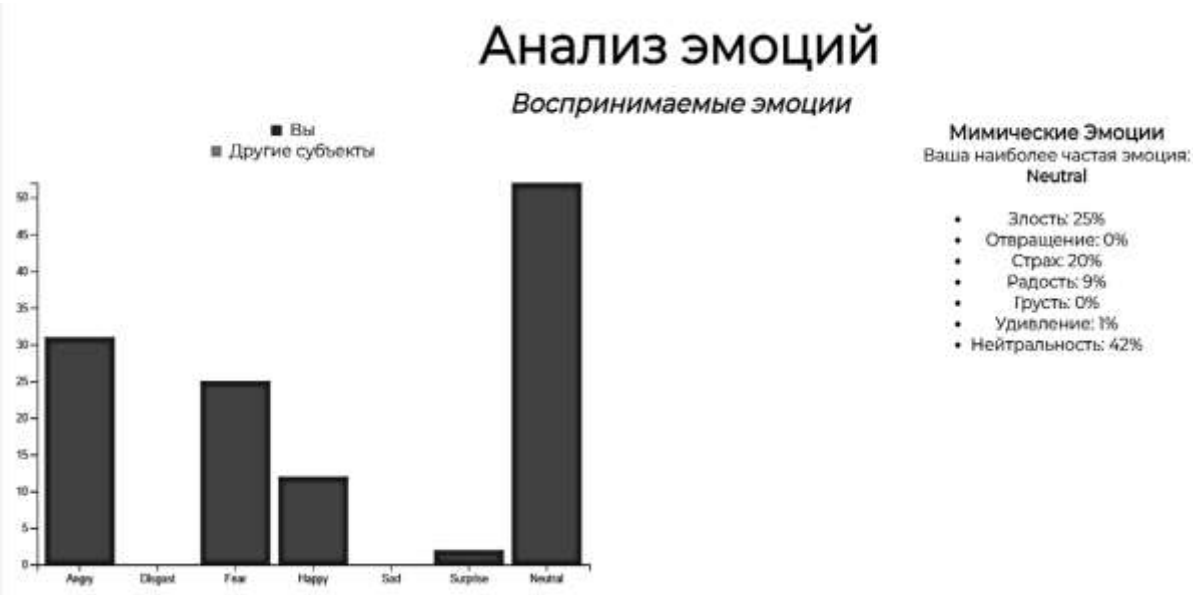


Рис. 4. Панель результатов распознавания эмоций пользователя

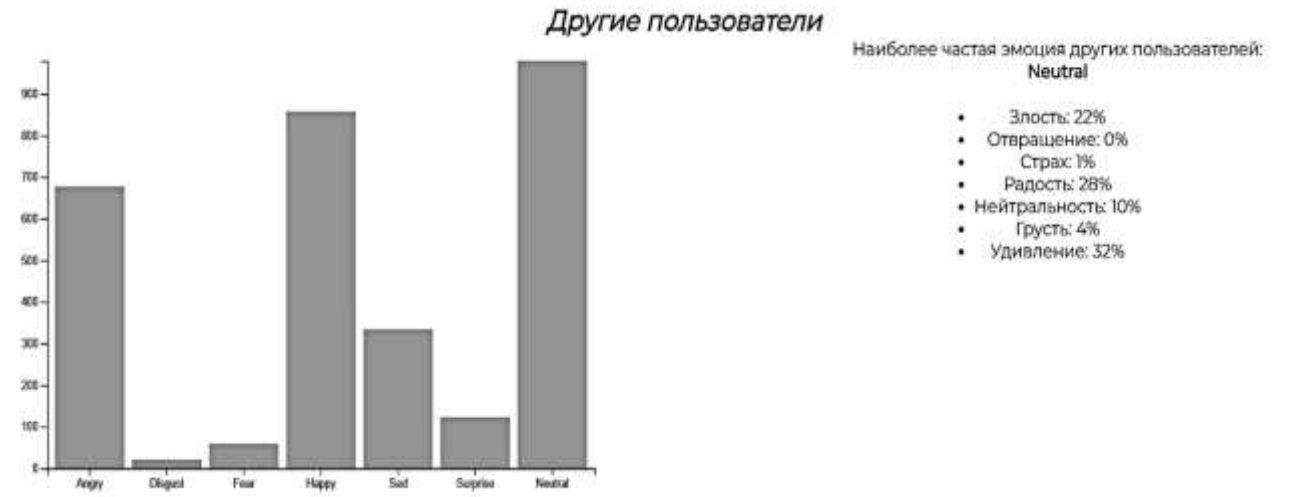


Рис. 5. Панель результатов распознавания эмоций пользователя

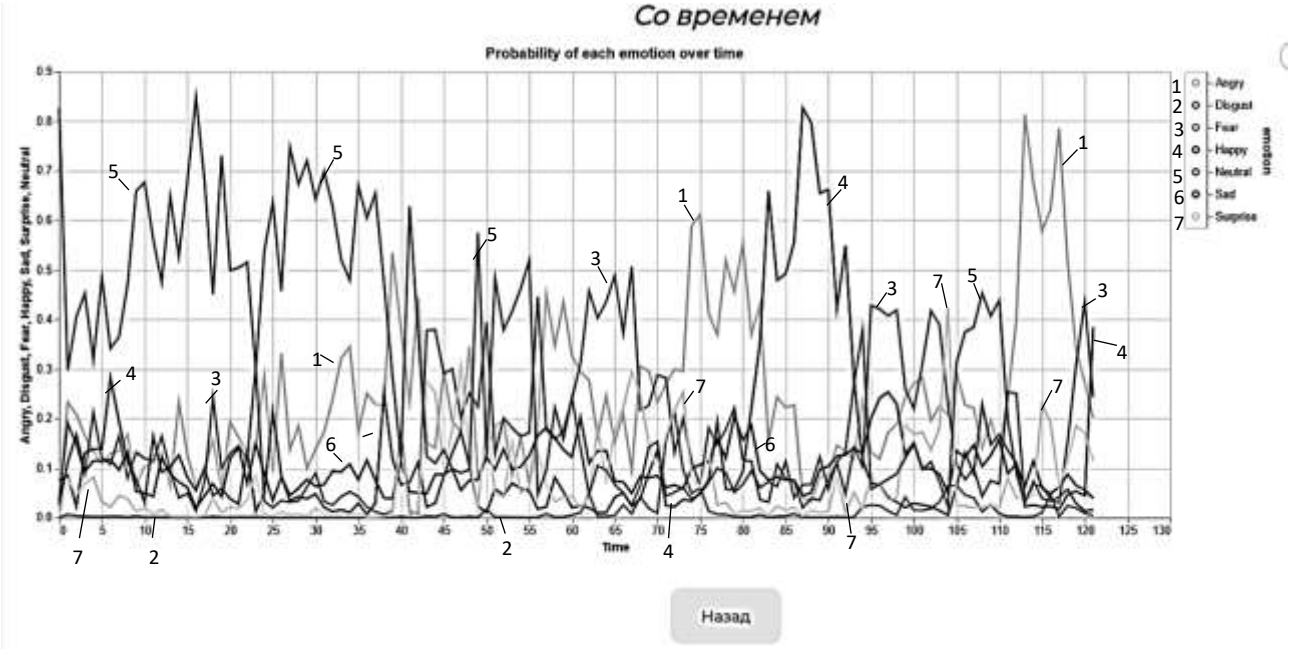


Рис. 6. Изменение эмоций пользователя в течении времени

Также для разработки модуля распознавания оружия (ножи, пистолеты, гранаты, ракеты, винтовки) используется набор данных, состоящий из 9633 изображений. Сама модель была обучена в YOLOv8 — это серия алгоритмов обнаружения объектов в реальном времени. YOLOv8 поддерживает следующие задачи и модели: обнаружение, сегментация экземпляров, поза/ключевые точки, классификация [15].

Архитектура данного модуля состоит из следующих элементов:

1. Базовая Сеть (Backbone) – это та часть архитектуры, которая отвечает за первоначальное извлечение признаков из входных данных.

2. Слои Обнаружения (Detection Layers): Эти слои отвечают за предсказание ограничивающих рамок, классов объектов и вероятности присутствия объектов в этих рамках;

3. Механизмы Интеграции Масштабов (Scale Integration Mechanisms): YOLO использует несколько масштабов для обнаружения объектов разного размера.

4. Функции Активации и Нормализации: Современные архитектуры нейронных сетей часто используют усовершенствованные функции активации и

нормализации для улучшения процесса обучения и эффективности сети;

4.1. Функции активации;

4.1.1. Leaky ReLU (Rectified Linear Unit): Эта функция активации используется в предыдущих версиях YOLO и характеризуется небольшим положительным уклоном в отрицательной части её графика. Помогает избежать проблемы "умирающего нейрона", которая возникает в стандартной функции ReLU (рис. 7).

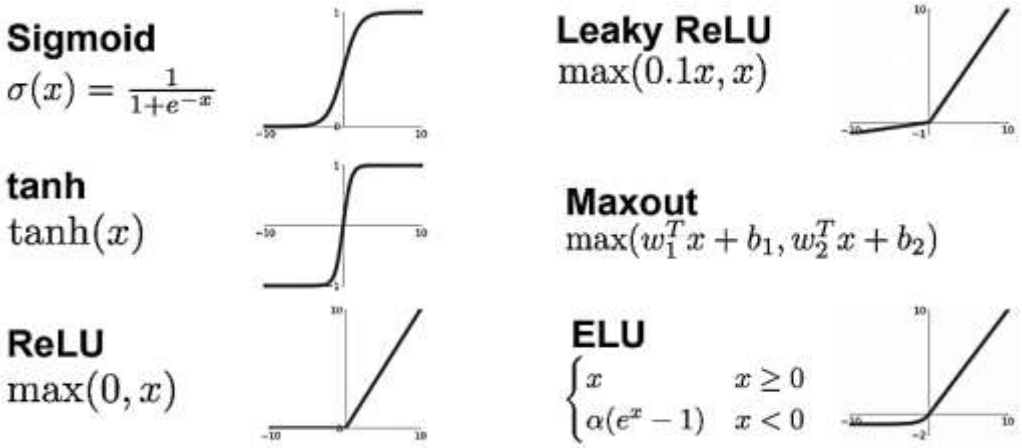


Рис. 7. Часто используемые функции активации в нейронных сетях

4.1.2. Mish или Swish: это новые функции активации, которые демонстрируют хорошие результаты в глубоком обучении за счет более гладкого перехода по сравнению с ReLU и Leaky ReLU. Они могут быть использованы для улучшения производительности сети.

4.2. Функции Нормализации;

4.2.1. Batch Normalization. Нормализует выход каждого слоя по мини-пакетам, что помогает уменьшить внутренний сдвиг ковариации;

4.2.2. Group Normalization или Layer Normalization: Эти методы могут быть альтернативой Batch Normalization, особенно в условиях, когда размер мини-пакета мал или когда сеть должна быть более стабильной при различных размерах пакетов;

4.2.3. Weight Normalization: Этот метод также может использоваться для улучшения скорости сходимости обучения, нормализуя веса нейронов.

Итоговая модель обучалась на наборе изображений размерностью 640x640 пикселей с количеством эпох, равным 20, и количеством партий, равным 16. Результаты обучения модели представлены на рис. 8.

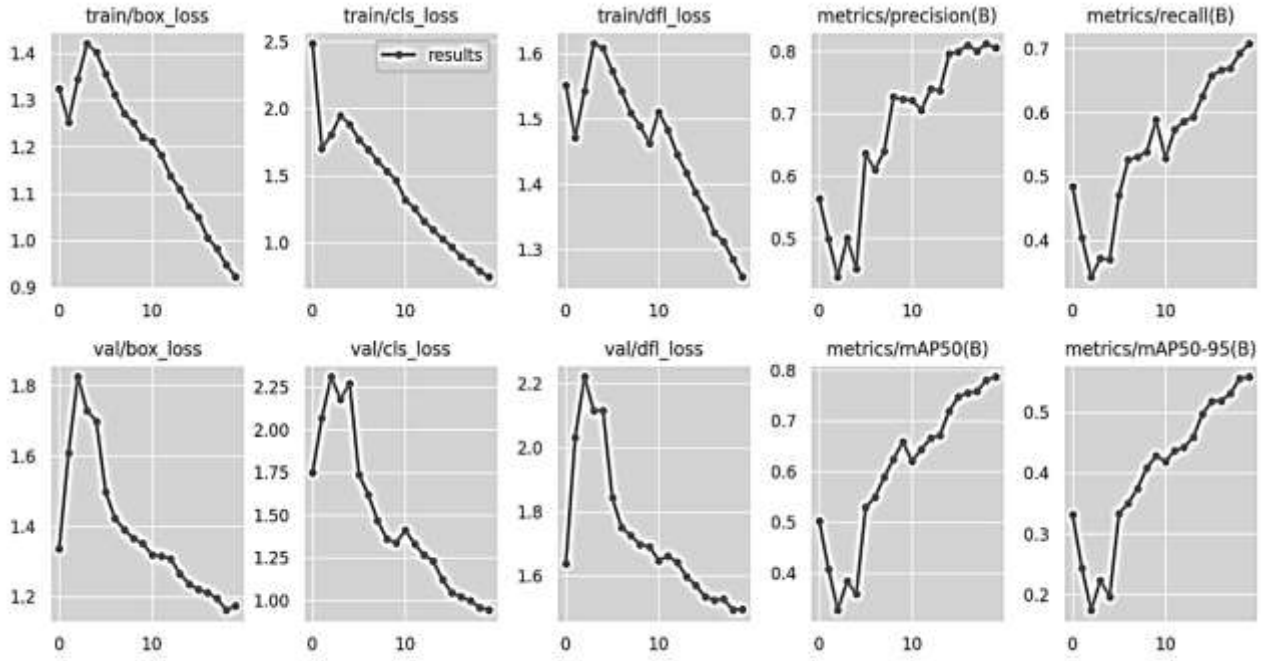


Рис. 8. Результат обучения модели

Из рис. 8 следует:

1. Потери (Loss);

1.1. Box Loss (Потери рамки ограничения): Значения потерь на тренировочном наборе данных (train) и валидационном (val) падают, что указывает на то, что модель улучшает свою способность точно локализовать объекты в рамках изображения.

1.2. Classification Loss (Потери классификации): также наблюдается снижение потерь классификации как на тренировочных, так и на валидационных данных, что указывает на улучшение точности классификации объектов моделью.

1.3. Direction/Focal Loss (Потери направления/фокальные потери): Потери уменьшаются, что указывает на улучшение в определении ориентации объектов (если это применимо к используемой модели).

2. Метрики качества (Metrics):

2.1. Precision (B): показывает долю правильно идентифицированных объектов среди всех объектов, которые модель идентифицировала как объекты данного класса (оружие). Наблюдается общий рост точности.

2.2. Recall (B): отражает долю правильно идентифицированных объектов класса (оружие) среди всех реальных объектов этого класса в данных. Рост показателя отражает способность модели находить больше реальных объектов.

2.3. mAP50 (B): Средняя точность по всем классам при пороге IoU в 0.5 (Intersection over Union – это метод для измерения точности алгоритмов обнаружения и сегментации объектов). Увеличение этой метрики говорит о повышении общей точности модели.

2.4. mAP50-95 (B): Средняя точность по всем классам, усредненная по диапазону порогов IoU от 0.5 до 0.95. Рост этой метрики указывает на то, что модель хорошо работает на различных уровнях строгости критериев совпадения.

**Заключение**

Перспектива применения создаваемого инструментария видится в том, что корпорациям предоставляются дополнительные возможности практически в реальном времени осуществлять мониторинг психофизического состояния их сотрудников на основе текущего анализа мимических эмоций. Подобное исследование (на основе видео с рабочего места) может реализоваться ежечасно, ежедневно и т.д. (в зависимости от критичности для корпорации занимаемой сотрудником должности и исполняемых им служебных обязанностей). Всё это будет создавать базу данных, характеризующих

эмоциональные состояния, рассматриваемого сотрудника в период мониторинга. Отсюда представляется возможность статистических оценок и выработки рекомендаций ЛПР, которое управляет доступом к корпоративной информации. Нейросетевая реализация позволит предложить интеллектуальные подсказки руководству компании по регламентации её деятельности с учётом текущего и системного психофизических состояний её персонала (т.е. с учётом психофизического портрета подчинённых и влияния человеческого фактора.

**Список литературы**

1. General strain theory (Общая теория напряжения) – URL: https://en.wikipedia.org/wiki/General_strain_theory (Дата обращения 09.11.2023)

2. MorphCast – URL: https://www.morphcast.com/ (Дата обращения 09.11.2023)

3. ITV “Face-Интеллект” – URL: https://www.itv.ru/company/press_centre/news/3144 (Дата обращения 09.11.2023)

4. FaceReader – URL: https://www.noldus.com/facereader (Дата обращения 09.11.2023)

5. Allcontrol – URL: https://www.allcontrol.rs/en/ (Дата обращения 09.11.2023)

6. Emotions in Criminal Decision Making / Jean-Louis Van Gelder – 2016. – 14 с.

7. Fear and Anger: Similarities, Differences, and Interaction – URL: https://www.psychologytoday.com/gb/blog/overcoming-destructive-anger/202103/fear-and-anger-similarities-differences-and-interaction (Дата обращения 12.11.2023)

8. Solomon R. C. (1993). The Passions: Emotions and the Meaning of Life. Hackett Publishing.

9. How Fear Leads to Anger – URL: https://www.psychologytoday.com/us/blog/hot-thought/201811/how-fear-leads-anger (Дата обращения 12.11.2023)

10. Ekman, P., & Friesen, W. V. (1978). Facial Action Coding System: A Technique for the Measurement of Facial Movement. Palo Alto: Consulting Psychologists Press.

11. FACS система кодирования выражений лица – URL: https://srccs.su/facs-sistema-kodirovaniya-vyrazhenij-litsa/ (Дата обращения 12.11.2023)

12. De Silva, L. C., Miyasato, T., and Nakatsu, R. Facial Emotion Recognition Using Multimodal Information. In Proc. IEEE Int. Conf. on Information, Communications and Signal Processing (ICICS'97), Singapore, pp. 397-401, Sept.1997.”

13. Xception: Deep Learning with Depthwise Separable Convolutions – URL: https://arxiv.org/abs/1610.02357 (Дата обращения 16.11.2023)

14. FER-2013 – URL: https://www.kaggle.com/datasets/msambare/fer2013 (Дата обращения 16.11.2023)

15. YOLOv8 – URL: https://github.com/ultralytics/ultralytics (Дата обращения 16.11.2023)

Воронежский государственный технический университет
Voronesh State Technical University

Поступила в редакцию 15.11.2023

**Информация об авторах**

**Остапенко Александр Григорьевич** – д-р техн. наук, профессор, заведующий кафедрой, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Зимницкий Андрей Григорьевич** – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Москалева Екатерина Алексеевна** – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

# GOAL-SETTING OF THE PROJECT ACTIVITY ON CREATION OF TOOLS FOR AUTOMATING THE DETECTION AND REGULATION RISKS OF DEVIANT BEHAVIOR OF CORPORATE EMPLOYEES

**A.G. Ostapenko, A.G. Zimnitsky, E.A. Moskaleva**

Based on a comprehensive study of the subject area, the relevance of creating tools for identifying and regulating the risks of deviant behavior of corporate employees in the context of ensuring their safety is substantiated. Consideration of analogues allowed to realize the goal-setting of project activities according to the line of mutually one-valued correspondence of the revealed contradictions, set tasks, expected results, their novelty, practical value and theoretical significance. In accordance with the above, the architecture of the created toolkit including various libraries and modules is proposed, their use is demonstrated on practical examples of automated analysis of human facial emotions (anger, disgust, fear, joy, sadness, surprise, etc).

Key words: risk, deviant behavior, corporation, goal setting, emotions.

Submitted 15.11.2023

**Information about authors**

**Aleksandr G. Ostapenko** – Dr. Sc. (Technical), Professor, Head of Department, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**Andrey G. Zimnitskiy** – Student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**Ekaterina A. Moskaleva** – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com