

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт инженерной и экологической безопасности

(наименование института полностью)

20.03.01 Техносферная безопасность

(код и наименование направления подготовки, специальности)

Безопасность технологических процессов и производств

(направленность (профиль)/специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему Биометрический контроль доступа в организации

Обучающийся

А.А. Саенко

(Инициалы Фамилия)

(личная подпись)

Руководитель

д.с.-х.н., доцент, Н.В. Шелепина

(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Консультант

к.э.н., доцент, Т.Ю. Фрезе

(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2025

Аннотация

Тема: «Биометрический контроль доступа в организации».

В разделе «Нормативные требования в области идентификации персонала» представлен анализ действующих нормативных требований к биометрическому контролю.

В разделе «Анализ современных биометрических технологий» проводится анализ сильных и слабых сторон биометрических технологий, особенности применения для контроля доступа и оценивается роль биометрических технологий в обеспечении безопасности производственных объектов.

В разделе «Совершенствование контроля доступа в организации» предлагаются технические решения, направленные на реализацию разработанной модели биометрической системы контроля доступа в организации и оцениваются преимущества разработанной модели биометрической системы контроля доступа по сравнению с мерами контроля доступа, действующими в организации.

В разделе «Охрана труда» производится оценка уровней профессионального риска на рабочих местах предприятия.

В разделе «Охрана окружающей среды и экологическая безопасность» определена антропогенная нагрузка предприятия на окружающую среду и оформлены результаты производственного экологического контроля по предприятию.

В разделе «Защита в чрезвычайных и аварийных ситуациях» представлены мероприятия по предупреждению ЧС на предприятии.

В разделе «Оценка эффективности мероприятий по обеспечению техносферной безопасности» выполнена оценка эффективности разработанных мероприятий по обеспечению техносферной безопасности.

Количественная характеристика: объем работы составляет 71 страницу, 3 рисунка, 20 таблиц.

Содержание

Введение	4
Термины и определения.....	6
Перечень сокращений и обозначений	7
1 Нормативные требования в области идентификации персонала	8
2 Анализ современных биометрических технологий	13
3 Совершенствование контроля доступа в организации.....	33
4 Охрана труда	39
5 Охрана окружающей среды и экологическая безопасность	46
6 Защита в чрезвычайных и аварийных ситуациях	54
7 Оценка эффективности мероприятий по обеспечению техносферной безопасности	59
Заключение	65
Список используемых источников	68
Приложение А Паспорт безопасности	72

Введение

Актуальность биометрического контроля доступа в организации продиктована высокими требованиями обеспечения безопасности опасных производственных объектов.

В современном мире технологическое оборудование взяло на себя задачи управления, ранее выполнявшиеся людьми, и автоматизация распространилась почти на все аспекты жизни. Возникла все более острая необходимость в надежной системе идентификации личности для проверки личности пользователей перед предоставлением им доступа в зоны ограниченного доступа или отклонением подделок. Как прямой результат этого, например, когда человек получает несанкционированный доступ к паролю, то традиционные методы проверки, которые полагаются на пароли, уязвимы для взлома. Поэтому для целей индивидуальной идентификации было разработано множество биометрических методов.

Химическая промышленность сегодня становится все более автоматизированной с появлением программируемых электронных систем измерения и контроля. Хотя повышенная автоматизация, включая системы сигнализации, управления и блокировок, снижает вероятность ошибок оператора, в автоматизированной системе управления могут возникать новые типы неисправностей. Сложность компьютерных измерительных систем увеличивает вероятность ошибок при проектировании и обслуживании. Для обеспечения высокого уровня безопасности руководство предприятия, опытный эксплуатационный персонал, специалисты по технологическим процессам, специалисты по безопасности и специалисты по проектированию контрольно-измерительных приборов и систем управления должны сотрудничать, обладая общими знаниями ключевых принципов и вопросов безопасности.

Цель исследования – повышение эффективности контроля доступа в организации за счёт реализации биометрических технологий в обеспечении

безопасности производственных объектов.

Задачи:

- провести анализ действующих нормативных требований к биометрическому контролю;
- представить особенности биометрического контроля персонала;
- представить классификацию современных биометрических технологий;
- проанализировать сильные и слабые стороны биометрических технологий, особенности применения для контроля доступа;
- оценить роль биометрических технологий в обеспечении безопасности производственных объектов;
- охарактеризовать структуру биометрической системы;
- оценить достаточность и эффективность действующей в организации системы контроля доступа;
- предложить модель биометрической системы контроля доступа в организации, основанную на одной из биометрических технологий;
- предложить конкретные технические решения, направленные на реализацию разработанной модели биометрической системы контроля доступа в организации;
- оценить преимущества разработанной модели биометрической системы контроля доступа по сравнению с мерами контроля доступа, действующими в организации;
- оценить антропогенное воздействие предприятия на окружающую среду;
- разработать паспорт безопасности на объект;
- оценить экономический эффект от реализации предложенных мероприятий.

Термины и определения

Загрязнение окружающей среды – «поступление в окружающую среду вещества и (или) энергии, свойства, местоположение или количество которых оказывают негативное воздействие на окружающую среду» [7].

Оценка воздействия на окружающую среду – «вид деятельности по выявлению, анализу и учету прямых, косвенных и иных последствий воздействия на окружающую среду планируемой хозяйственной и иной деятельности в целях принятия решения о возможности или невозможности ее осуществления» [7].

Оценка профессиональных рисков – «это выявление возникающих в процессе осуществления трудовой деятельности опасностей, определение их величины и тяжести потенциальных последствий» [20].

Производственные объекты – объекты промышленного и сельскохозяйственного назначения, в том числе склады, объекты инженерной и транспортной инфраструктуры (железнодорожного, автомобильного, речного, морского, воздушного и трубопроводного транспорта), объекты связи.

Перечень сокращений и обозначений

АПФД – аэрозоли преимущественно фиброгенного действия.

АСОДУ – автоматизированная система оперативного диспетчерского управления.

АСУТП – автоматизированная система управления технологическим процессом.

ИИ – искусственный интеллект.

КИПиА – контрольно-измерительные приборы и автоматика.

НТД – нормативно-техническая документация.

ПАЗ – противоаварийная защита.

ПДК – предельно-допустимая концентрация.

СИЗ – средство индивидуальной защиты.

СКУД – система контроля и управления доступом.

ФГУП – федеральное государственное унитарное предприятие.

ЧОП – частное охранное предприятие.

3DFR – трехмерное распознавание лиц.

ASR – автоматическое распознавание речи.

MES (Manufacturing Execution System) – программное обеспечение, которое предназначено для управления и контроля производственными процессами в реальном времени на предприятии.

1 Нормативные требования в области идентификации персонала

Биометрическая идентификация очень надежна, поскольку гораздо сложнее подделать физические черты, чем коды безопасности, пароли, аппаратные ключи, датчики, быстродействующее оборудование и большой объем памяти. Однако система дорогая. Некоторые из применений биометрической идентификации включают сетевой и рабочий доступ, вход в приложения с одним паролем, защиту данных, удаленное использование ресурсов, безопасность транзакций и веб-безопасность. Надежные процессы идентификации личности могут помочь электронной коммерции и электронному правительству оправдать свои перспективы. Люди уже используют эти технологии для безопасного онлайн-банкинга, инвестирования и других финансовых операций. Они также полезны для продаж в магазинах, правоохранительных органов, здравоохранения и социальных служб и многого другого. Биометрические технологии, вероятно, будут очень важны для обеспечения доступа к крупным деловым сетям только уполномоченных лиц. Они также будут использоваться в точках продаж для защиты всех видов цифровых материалов, например, в управлении цифровыми правами, а также в учреждениях здравоохранения. Ожидается, что биометрия будет использоваться практически в каждой части бизнеса и нашей повседневной жизни. Ее можно использовать как отдельно, так и вместе с другими технологиями, такими как смарт-карты, ключи шифрования и цифровые подписи [4].

Развертывание надежной системы аутентификации пользователей стало ключевой обязанностью, как для контроля доступа, так и для защиты личных данных пользователей в связи с быстрым ростом электронных преступлений и связанных с ними трудностей.

Федеральный закон от 27.07.2006 № 149-ФЗ определяет порядок защиты личной и биометрической информации [8].

Требования Федерального закона от 27.07.2006 № 152-ФЗ (ред. от

08.08.2024) «О персональных данных» [6] направлены на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Постановление Правительства РФ от 30.06.2018 № 772 (ред. от 12.07.2022) «Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты» [9] определяет состав сведений в единой биометрической системе.

В своих разъяснениях Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30.08.2013 «Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки» [18] объясняет основные положения по работе с биометрическим персональным данным человека.

В соответствии с ч. 1 ст. 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» [6] к биометрическим персональным данным относятся сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

Соответственно, в контексте Федерального закона «О персональных данных» отнесение сведений персонального характера к биометрическим персональным данным и их последующая обработка должны рассматриваться в рамках проводимых оператором мероприятий, направленных на

установление личности конкретного лица, если иное не предусмотрено федеральными законами и принятыми на их основе нормативными правовыми актами.

Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных ч. 2 ст. 11 Федерального закона «О персональных данных», [6] предусматривающей исключения, связанные с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

Исходя из определения, установленного Федеральным законом «О персональных данных» [6] к биометрическим персональным данным относятся физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и другие), а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности субъекта.

Проблемы конфиденциальности: сбор и хранение биометрических данных может вызвать серьезные проблемы конфиденциальности. Если базы данных биометрических данных будут взломаны, конфиденциальная информация людей может быть раскрыта, что приведет к краже личных данных или другим вредоносным действиям.

Как для частного, так и для публичного использования биометрические

характеристики человека, включая голос, палец, сканирование радужной оболочки глаза, лицо, подпись и другие характеристики, обеспечивают надежный уровень безопасности.

Физиологические или поведенческие характеристики человека используются биометрическими системами идентификации личности для целей распознавания, где речь, почерк, нажатия клавиш являются поведенческими чертами, в то время как отпечатки пальцев, лица и геометрия руки являются физиологическими чертами.

Растущая потребность в установлении и проверке достоверной личной идентичности во многих государственных и частных секторах привела к огромному развитию технологии биометрической аутентификации в последние годы.

Биометрия относится к изучению и практике идентификации людей на основе их уникальных физиологических и поведенческих черт. Биометрическая аутентификация набирает обороты во многих областях, включая банковское дело, авиацию, финансовые транзакции, доступ в различные здания и помещения.

Два компонента, регистрация и тестирование, являются основой такой системы. Хранение шаблона в базе данных происходит во время процедуры регистрации. Кроме того, во время тестирования собранные шаблоны сравниваются с данными от людей.

Сопоставляющее программное обеспечение использует соответствующий алгоритм для сравнения ввода и шаблона, и оценки расстояния между ними.

Чтобы использовать распознавание биометрических признаков для облегчения идентификации человека, пользователи должны сначала загрузить фотографию объекта в систему. Затем система повторно обработает изображение, удалив шум и другие нежелательные аспекты [1].

Следующий шаг – система использует ориентиры изображения, включая такие факторы, как расстояние между глазами, длина линии челюсти и так

далее, для определения классификации изображения. Затем система отображает результаты своего поиска по базе данных, которые она ранее определила как идеальное совпадение.

Вывод по разделу.

В разделе определено, чтобы гарантировать, что организационные и/или личные данные хорошо хранятся и доступны только назначенной стороне, необходимо реализовать защищенную биометрическую инфраструктуру. Крайне важно, чтобы был способ проверки только тех людей, которые определены как работники организации.

Особенностями биометрического контроля персонала заключается в том, что биометрические данные могут с вероятностью близкой к 100 % идентифицировать персонал в тех случаях, когда это необходимо для обеспечения безопасности.

2 Анализ современных биометрических технологий

Биометрия – это изучение человеческих характеристик с целью разработки надежных методов идентификации личности. Ожидается, что этот подход превзойдет более традиционные способы, используемые ранее.

Эффективность системы в реальных сценариях может быть измерена путем сравнения соотношения ложных положительных и ложных отрицательных результатов. Для использования в системе в качестве биометрических признаков биометрический идентификатор должен соответствовать определенным критериям:

- отличительная черта: каждый человек по-своему оригинален;
- получение ответственности: возможность может быть получена быстро и без необходимости интенсивной обработки для каждого отдельного случая;
- возможность высокого разрешения: два человека по своей сути неотличимы друг от друга;
- устойчивость: устойчивость во времени и окружающей обстановке, характеристики не меняются.

Биометрические приложения в значительной степени полагаются на человеческие аспекты, такие как обучение моделей искусственного интеллекта (далее – ИИ) с высокой степенью обучения и процессов обучения, которые, в свою очередь, обучают всю модель отражать человеческие взгляды и черты с точки зрения человеческих характеристик, таких как лицо, отпечатки пальцев, губы или радужная оболочка глаза, или ладонь руки, или даже язык, который является частью системы идентификации человека [1].

Первая часть конструкции, датчик, собирает данные из внешнего мира и функционирует как связующее звено между системой и фактической средой. Он универсален и может адаптироваться ко многим приложениям, но системы захвата изображений на основе компьютерного зрения хорошо подходят. Второй блок отвечает за предварительную обработку, которая включает

улучшение входного изображения и удаление артефактов с датчика. Последующий раздел отвечает за извлечение ключевых атрибутов. Оптимальное извлечение правильных характеристик изображения имеет важное значение на этом этапе. Чтобы создать шаблон, используются либо характеристики изображения, либо вектор чисел, которые имеют определенные характеристики. Извлеченный набор схожих характеристик из источника объединяется для формирования шаблона. Шаблоны используются для уменьшения размера файла и сохранения личности в памяти. Уменьшение размера производится путём устранения элементов биометрических мер, которые не нужны для алгоритмов сравнения [2].

Рассмотрим различные типы биометрических признаков.

Физиологический анализ биометрии состоит из лица, отпечатков пальцев, геометрии руки, радужной оболочки глаза, ДНК, сканирования сетчатки глаза, распознавания вен глаз, распознавания лица, распознавания вен пальцев, распознавания отпечатков ладоней, распознавания вен ладоней, распознавания термографии и поведенческого анализа, динамики нажатия клавиш, жестов, голоса (речевых сигналов), походки (обнаружения движения), распознавания говорящего, движения губ.

Чтобы идентифицировать преступление и преступника, используются процедуры обнаружения отпечатков пальцев, но в наши дни для этого создана механизированная система.

Распознавание отпечатков пальцев. Одним из важных методов в судебной экспертизе является извлечение частичных отпечатков пальцев с места преступления. Отпечатки пальцев, оставленные на металлических или стеклянных поверхностях, вызваны сочетанием жира и влаги на пальце [3].

Пики ребристых отпечатков кожи могут использоваться для переноса чернил или других веществ на гладкую поверхность, например, бумагу, чтобы намеренно оставить полный отпечаток пальца. Хотя карты отпечатков пальцев обычно также захватывают части нижних суставных областей пальцев, записи отпечатков пальцев обычно содержат отпечатки с подушечки на конечном

суставе пальцев и больших пальцев.

Отпечатки пальцев человека детализированы, почти уникальны, их трудно изменить, и они долговечны в течение жизни человека, что делает их пригодными в качестве долгосрочных маркеров человеческой личности. Они могут использоваться полицией или другими органами для идентификации лиц, которые хотят скрыть свою личность, или для идентификации людей, которые недееспособны или умерли и, таким образом, не могут идентифицировать себя. Сопоставление двух отпечатков пальцев является одним из наиболее используемых и надежных биометрических методов.

Сопоставление отпечатков пальцев просто учитывает видимые характеристики отпечатка пальца.

Существуют два метода обнаружения отпечатков пальцев: сопоставление образов на основе зрения для идентификации и обнаружение мелких деталей (таких как окончания гребней, разветвления, точки или острова).

Автоматизированный процесс сопоставления введенного отпечатка пальца с сохраненным шаблоном отпечатка пальца для идентификации человека известен как распознавание отпечатков пальцев. Несмотря на то, что распознавание отпечатков пальцев существует уже некоторое время, в настоящее время оно является одной из наиболее используемых биометрических характеристик.

При сопоставлении с образцом два изображения анализируются для определения их сходства, тогда как подходы, основанные на мелких деталях, полагаются на определение местоположения и ориентации мелких деталей.

Хотя распознавание радужной оболочки глаза все еще остается довольно редким видом биометрической идентификации, в ближайшие годы мы можем ожидать более широкого его использования [4].

Поскольку каждая радужная оболочка отличается от другой, они являются идеальным инструментом биометрической верификации.

Одной из областей, которая, как ожидается, будет развиваться с более

широким использованием распознавания радужной оболочки глаза, является иммиграционный контроль, как мера предосторожности и реакция на глобальную опасность терроризма.

Распознавание радужной оболочки глаза является широко востребованным методом идентификации, особенно в таких областях, как пограничный контроль и правоохранительные органы, поскольку это очень надежная биометрия с высокой скоростью поиска по большим наборам данных и чрезвычайно устойчивая к ложным совпадениям. Распознавание радужной оболочки глаза является мощным и невероятно надежным методом для точной идентификации людей [5].

Различные методы распознавания радужной оболочки могут включать получение изображений, определение их местоположения, сегментацию и последующее сопоставление. Для получения изображения радужной оболочки с высоким разрешением, необходимого для аутентификации, можно использовать камеру с высокой частотой кадров или оборудование для видеосъемки. Выполнение фазы локализации следует за получением изображения радужной оболочки. Этот метод определяет область радужной оболочки на изображении. Граница радужная оболочка/склера (внешняя) и граница радужная оболочка/зрачок (внутренняя) – это два круга, которые можно использовать для аппроксимации этого.

Сегментация, следующий шаг после локализации радужной оболочки, заключается в разделении входного изображения радужной оболочки на множество частей. Последний этап после сегментации и локализации радужной оболочки – сопоставление с образцом с использованием шаблонов базы данных.

Развитие радужной оболочки начинается на третьем месяце эмбрионального развития и почти завершается к восьмидесяти первому месяцу. Мы можем извлечь схожие характеристики из радужной оболочки благодаря ее сложному виду и структуре. Хотя визуализация поверхности радужной оболочки не очень сложна, тем не менее, это то, о чем следует тщательно

подумать. Вероятность ошибки увеличивается, например, при работе с изображениями, у которых были скорректированы контраст, разрешение и фокус, или при просмотре их глазами, углы вращения которых смещены. Также возможно обнаружить идентификацию с помощью этой стратегии.

Цвет и текстура радужной оболочки глаза человека могут значительно различаться от человека к человеку.

Поэтому сканирование радужной оболочки глаза человека является подходящим средством идентификации. В этой технике используется сканирование цветной области глаза [5].

Распознавание сетчатки – это биометрический метод, который идентифицирует человека на основе различных узоров на сетчатке. Слой кровеносных сосудов в задней части глаза называется сетчаткой. Глаз помещается перед аппаратом на расстоянии до одного метра (8 см) для захвата. Задача требует от пользователя выровнять последовательность маркеров, которые видны через окуляр. Чтобы сканер записал узор сетчатки, глаз должен быть оптически сфокусирован. Ближний инфракрасный свет на длине волны 890 нм сканирует сетчатку для идентификации отчетливого узора кровеносных сосудов. Уникальность узоров кровеносных сосудов используется при распознавании сетчатки. Коммерческая разработка началась в середине 1970 гг. По данным Sandia Laboratory, менее 1,0 % отклонений были неверными.

Для человеческого глаза сетчатка является аналогом пленки для фотоаппарата. Она преобразует свет в электрические импульсы благодаря миллионам своих фоторецепторов.

Метод идентификации на основе сетчатки использует преимущество характерного расположения кровеносных сосудов сетчатки. Поскольку сетчатка расположена на задней стороне глаза, она остается стабильной на протяжении всей жизни человека, несмотря на то, что не видна напрямую. Необходимость в инфракрасном источнике света для освещения сетчатки дополнительно обоснована по этой причине. Одним из преимуществ

инфракрасного света является то, что кровеносные сосуды сетчатки поглощают его с гораздо большей скоростью, чем остальная ткань глаза. А затем сканирующее устройство принимает весь этот отраженный свет и обрабатывает его. Получение, обработка, сопоставление и представление изображения в виде шаблона – все это этапы процесса сканирования сетчатки. По сравнению с другими биометрическими методами размер шаблона довольно мал, обычно 96 байт.

Для сканирования сетчатки глаза человеку необходимо снять очки, поднести глаз к сканеру, сфокусироваться на фиксированной точке и оставаться неподвижными в течение 10-15 секунд, пока происходит сканирование [4], что является недостатком технологии, если необходимо идентифицировать работника быстро.

Распознавание вен руки или пальца. Сопоставление вен, также известное как сосудистая технология или биометрия вен пальцев, является методом биометрической аутентификации, который исследует узоры кровеносных сосудов, видимых через поверхность кожи. Этот метод использует ближний инфракрасный свет, чтобы осветить на пальцы человека, чтобы сделать снимки вен внутри его руки. В результате его практически невозможно подделать. Кроме того, наличие крови в венах во время идентификации подтверждает, что идентифицируемый человек является реальным и живым.

Сосудистые рисунки руки пользователя являются основным объектом внимания систем идентификации вен. Технология аутентификации вен обеспечивает высокую степень точности по сравнению с другими биометрическими системами, поскольку вены пользователя находятся внутри человеческого тела, что делает их копирование невозможным.

Серия светодиодов, излучающих свет в ближнем инфракрасном диапазоне, создает изображение, проникая в кожу руки и заставляя свет поглощаться кровеносными сосудами. База данных биометрического устройства строится из множества шаблонов, которые создаются из этого цифрового изображения. Шаблоны могут быть созданы с использованием

различных переменных, таких как расположение ветвей сосудов, толщина вен и углы ветвления. Возможны как контактные, так и бесконтактные типы оборудования для визуализации сосудов. Преимущество бесконтактного метода заключается в том, что человеку, предоставляющему биометрические данные, даже не нужно прикасаться к датчику. Это эффективно в ситуациях, когда требуется чрезвычайная чистота, в том числе в операционных для медицинских процедур, или когда люди боятся прикасаться к биометрическим датчикам [3].

Представлен новый подход к идентификации личности с использованием изображений сосудов. Системы контроля доступа, работающие в условиях покрытия сети, могут извлечь выгоду из этого подхода.

Регистрация, сбор данных и распознавание являются двумя фазами этого исследования. Используя ближнюю инфракрасную визуализацию, фаза регистратора собирает N изображений рук разных людей в рамках основной программы.

Для создания адаптивных образцов изображения проходят предварительную – обработку, извлечение признаков и моделирование. Затем нейронная сеть используется для проверки.

Порог обнаружения изображения, обнаружение края, удаление края, извлечение скелета сосуда, улучшение разрешения с использованием морфологических функций составляют предварительную обработку в описываемом подходе.

После применения интегрированного преобразования изображения и статистическому извлечению признаков, необходимые векторы должны быть созданы на этапе извлечения признаков для сравнения на этапе аутентификации. Фактически, эта технология открыла новую эру в технологии идентификации, и ПЗС-камера может получить изображение только с помощью вены руки [5].

Распознавание лиц идентифицирует человеческие лица с помощью

биометрии и технологий, обычно с помощью искусственного интеллекта.

Хотя технология распознавания лиц может использоваться для подтверждения личности, также возникают проблемы с конфиденциальностью. Вот как это работает: программное обеспечение поставляется с минимум одним видео или фотографией, на которых изображено лицо человека.

Подпись лица – это карта черт лица человека, созданная программным обеспечением путем сканирования фотографий и видео. Она содержит информацию о точном положении глаз, шрамов и других черт лица.

Подпись лица пользователя сравнивается с базой данных с использованием технологий распознавания лиц.

В настоящее время в многочисленных базах данных можно найти десятки миллионов, а может быть, и миллиарды фотографий.

Соответствует ли подпись лица чему-либо в базе данных системы, определяется программным обеспечением распознавания лиц.

Некоторые системы могут дополнительно вычислять оценку точности или предлагать замены.

Одно из определений программного обеспечения для распознавания лиц – это приложение, которое может проверить личность человека, используя только фотографию или видеоклип. Картирование черт лица является основой этой техники. Картирование черт лица включает измерения таких вещей, как соотношение глаз и носа, ширина носа, длина линии челюсти. Для того чтобы количественно оценить эти точки, которые называются узловыми точками, генерируется числовой код, тем самым устанавливая уникальный отпечаток пальца для каждого человека. Лицо в базе данных представлено этим отпечатком пальца.

Автоматизированные системы распознавания лиц используют как 2D, так и 3D методы (рисунок 1).

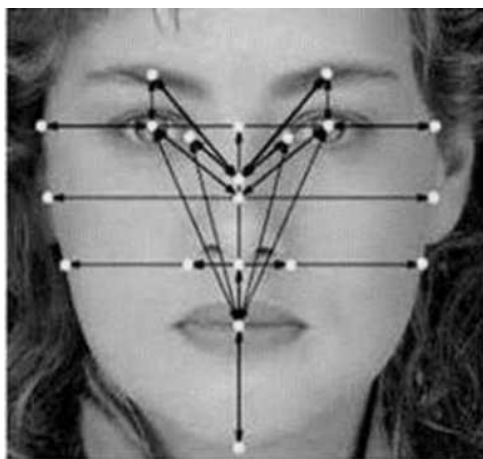


Рисунок 1 – Картирование черт лица

Рисунок 2 демонстрирует пример распознавания лиц в действии, которое включает идентификацию человеческого лица на основе его характерных линий и других характеристик. Обучение алгоритмов вычислений основано на отдельных и индивидуальных структурах каждого лица.

Технологии распознавания лиц 2D обнаруживают лица, сравнивая цифровые изображения, например, полученные камерой, содержащей терминал аутентификации распознавания лиц, биометрический планшет, а также смартфон, с базой данных ранее сделанных фотографий. Это наиболее часто используемый вид технологии распознавания лиц, поскольку он менее затратен и прост в применении, чем другие подходы.

Метод распознавания лиц 2D построен с использованием математической модели, которая извлекает информацию из цифровых изображений, чтобы различать узловые точки лица с их расстояниями на человеческом лице, такими как размер глаз или носа. Этот вид программного обеспечения для распознавания лиц, а также алгоритм работают путем сравнения черт лица внутри изображения с чертами в существующих наборах данных, что позволяет ему создавать идентификацию человека с точностью.

Алгоритм Eigenfaces, 2D Principal Component Analysis, Linear

Discriminant Analysis и другие подходы используются в 2D идентификации лиц. Каждая из этих систем распознавания лиц имеет свои отличительные качества и преимущества.

Трехмерное распознавание лиц (3DFR) стало мощным инструментом для идентификации людей по их лицам. Существует два основных принципа, когда речь идет о методах распознавания: традиционный и современный. В то время как последние в основном используют глубокое обучение для сквозного 3DFR, первые часто извлекают уникальные характеристики лица (например, глобальные, локальные и гибридные признаки) для сопоставления.

Одной из самых больших проблем распознавания лиц является его чувствительность к выражениям лица.

Это решается геометрической структурой для трехмерной идентификации лица, которая показана здесь.

Выражения лица, являющиеся неотъемлемой чертой человеческого лица, сложнее в управлении, чем внешние переменные, такие как освещение или поза.

Биометрические методы, основанные на поведенческих признаках человека. Поведенческая биометрия – это метод аутентификации пользователя, который собирает данные о действиях пользователя. Она отличается от физической биометрии, которая фокусируется на физически идентифицируемой информации (такой как отпечатки пальцев и распознавание лиц) для оценки человеческих качеств.

Каждый человек связан с определенным набором поведенческих атрибутов, которые известны как поведенческая биометрия. Анализируя действия пользователя в прошлом, поведенческая биометрия может обнаружить мошенническую деятельность и подтвердить его личность. Компании могут предложить более безопасный способ идентификации для человека с поведенческой биометрией, которая является пассивной, поскольку не требует никакой активности от пользователя. Поведенческая биометрия, ее применение, классификации и преимущества в контексте кибербезопасности

более защищены.

Поведенческая биометрическая техника также может быть разделена на три основных раздела:

- блок датчиков: отвечает за сбор биометрических данных;
- блок извлечения признаков: работает с собранными данными для определения их векторных признаков;
- блок сравнения: его задача – проверить полученный вектор на соответствие предопределенным шаблонам.

Распознавание динамических подписей. Динамическая подпись – это форма биометрической аутентификации, которая использует физические и поведенческие черты, которые человек демонстрирует, подписываясь именем или другим словом.

Существует разница между устройствами динамической подписи и системами считывания электронной подписи. Последняя используется для фотографирования подписи и широко распространена в местах, где предприятия собирают их для авторизации транзакций.

Для анализа почерка человека (динамическое распознавание подписи) используется множество признаков. Эти признаки собираются с помощью сенсорной технологии, включая цифровые планшеты или персональные цифровые помощники, и их использование и значение различаются у разных поставщиков оборудования.

Повседневная жизнь опирается на подписи людей для авторизации денежных транзакций, юридических документов, контрактов и многого другого. В какой-то момент этой процедуры внешний вид подписи был главной заботой. Один из способов взглянуть на это – сравнить подписи. Пользователи могут выполнить захват подписи в реальном времени с помощью динамического распознавания подписи, написав свою подпись на цифровом планшете, который связан с персональным компьютером для выполнения обработки и проверки [2]. Время, нажим при письме и скорость – все это поведенческие характеристики, присущие подписанию. Дублировать

визуальный вид подписи очень легко, но дублировать ее поведенческие качества довольно сложно. Типичные примеры динамических данных, используемых для целей распознавания, включают координаты x и y , давление, наклон, скорость и ускорение.

Для аутентификации личности пользователя на компьютере технология динамической проверки подписи использует поведенческие биометрические данные рукописной подписи. Для этого анализируются данные о форме, скорости, штрихе, давлении пера и времени процесса подписи.

Хотя подделать подпись просто, трудно «имитировать» поведенческие модели, присущие подписанию, что является главным преимуществом распознавания подписи. Распознавание подписи, напротив, имеет более высокий уровень ошибок, особенно когда поведенческие черты знаков противоречивы.

Статические подходы рассматриваются как двумерные изображения, лишённые зависящей от времени информации, которые служат подписью. В результате подпись может быть проверена с использованием ее статических, не зависящих от времени признаков. Следовательно, процесс распознавания подписей превращается в рутинную процедуру распознавания образов. Поскольку образец подписи неизбежно изменится, процедура проверки подписи этого метода может быть ограничена выявлением и картографированием области существенных изменений [6].

Вместо того, чтобы сравнивать подпись после того, как она была сделана, распознавание динамики знака зависит от динамики создаваемой подписи. Для оценки динамики используются давление, направление, ускорение и длина штрихов, а также количество и продолжительность штрихов. Наиболее очевидным и значительным преимуществом этого является то, что, взглянув на ранее созданную подпись, мошенник не может узнать, как ее написать. Динамика подписи регистрируется с помощью различных устройств.

Это либо специализированные гаджеты, либо обычные планшеты.

Методика обнаружения подписей изучает стиль письма пользователя. Этот подход оценивает режим изменения давления пера, а также случай письменных инструкций по осям X и Y. Датчики движения и давления находятся либо внутри пера, либо под бумагой для выполнения этого. Датчик определяет давление, направление и скорость, как описано ранее. Затем, по мере обработки данных, создается одновременный вектор, и данные из двух векторов сопоставляются. Две основные категории методов распознавания подписей – динамические (онлайн) и статические (офлайн).

Трехмерные движения могут быть записаны с помощью специализированных пишущих инструментов. У планшетов есть два основных недостатка. Первоначально оцифрованная подпись, которая создается, кажется отличной от типичной подписи пользователя. Во-вторых, пользователь не видит, что он ранее подписывался. Для многих – это существенный недостаток. Некоторые специальные ручки работают так же, как и обычные ручки.

Распознавание образов по голосу. Машины и программы с возможностями распознавания голоса или говорящего могут воспринимать и обрабатывать устные инструкции или диктовку. С распространением ИИ и умных помощников, таких как Siri и Alexa от Apple и Amazon, распознавание голоса стало более популярным и широко используемым.

Теперь клиенты могут заказывать вещи, устанавливать напоминания и выполнять другие простые действия по дому одним лишь голосом благодаря технологиям распознавания голоса.

С помощью программного обеспечения автоматического распознавания речи (ASR) голоса могут быть распознаны и дифференцированы. Чтобы получить максимальную отдачу от преобразования речи в текст, пользователи некоторых приложений ASR должны научить программное обеспечение распознавать их голос.

Системы автоматического распознавания речи анализируют темп, интонацию и рисунок голоса говорящего.

Термины «распознавание голоса» и «распознавание речи» иногда используются как взаимозаменяемые, однако между ними есть существенная разница. В то время как распознавание речи анализирует содержание произнесенных слов, распознавание голоса определяет, кто говорит.

Два фактора допускают возможность того, что голос человека может быть биометрической характеристикой. Прежде всего, голос – это физиологическое явление, возникающее в результате работы голосового тракта. Кроме того, это недостаток характера, который проявляется в форме акцента в голосе.

Когда складываются эти две вещи вместе, становится довольно сложно точно имитировать чужой голос. Звук в форме человеческой речи может быть преобразован в электрические импульсы с помощью технологии распознавания голоса. Для облегчения аутентификации эти сигналы кодируются. С помощью микрофона записываются произнесенные слова или фразы. Для расчета отношения правдоподобия входные образцы речи сравниваются с зарегистрированными моделями.

Системы распознавания также должны учитывать естественные изменения голоса человека с возрастом.

Кроме того, злоумышленники могут получить контроль доступа, записав голоса авторизованных пользователей, а затем пропустив запись через процедуру проверки. В процессе проверки системы распознавания речи потребуют от пользователей повторить ряд случайно сгенерированных слов, чтобы предотвратить незаконный доступ с использованием записывающего устройства.

Новая технология биометрической аутентификации – отпечаток языка, который является уникальным и сложным в подделке, поскольку не существует двух одинаковых отпечатков.

В биометрии человек мгновенно идентифицируется путем сравнения его уникальных физических или поведенческих черт с базой данных записей большого количества других людей. Одним из способов достижения этого

является использование биометрического сканирующего оборудования, такого как сканер отпечатков языка, который записывает уникальную биометрическую информацию пользователя, а затем оцифровывает ее для компьютерного анализа и проверки. Этот вид идентификации обеспечивает более надежную гарантию [2]. Форма и текстура открытого языка несут информацию, известную как отпечаток языка.

Физиологическая шероховатость поверхности языка и его геометрическая форма вполне постоянны [3]. В отличие от других форм идентификации, язык хорошо виден для осмотра и хорошо защищен от факторов окружающей среды, что делает его чрезвычайно сложным для изменения или подделки [4].

Исследования показали, что даже языки однояйцевых близнецов не выглядят в точности как друг у друга, что добавляет уникальности каждому индивидуальному отпечатку языка [5]. Существуют статические и динамические функции аутентификации, предоставляемые языком. Таким образом, биометрические системы идентификации, включающие отпечатки языка, быстро набирают популярность [1]. Система идентификации по отпечаткам языка была в центре внимания исследований в течение последних десяти лет.

Одним из надежных методов защиты конфиденциальной информации, хранящейся в цифровых форматах, является биометрическая аутентификация. По сравнению с более традиционными формами проверки, она обеспечивает превосходную безопасность и удобство. Проблемы с конфиденциальностью, ложные срабатывания и высокие цены – вот некоторые из недостатков.

Преимущества биометрических индикаторов:

- разница между ними и паролями в том, что они связаны с конкретным человеком;
- не придется беспокоиться о том, чтобы что-то носить с собой или помнить, что делает их очень удобными;
- они достаточно устойчивы к мошенничеству с точки зрения

безопасности;

- точная идентификация;
- простота использования;
- устойчивость к подделке;
- безопасность;
- масштабируемость

Технология на основе отпечатков пальцев: поскольку влажность оказывает большое влияние на емкость, она также влияет на битовую карту отпечатков пальцев, полученную со сканера. Из-за этого у людей с аномально влажными или сухими руками возникают проблемы с использованием этих считывателей отпечатков, поскольку создаваемые ими битовые карты недостаточно высокого качества.

Технология распознавания лиц: хотя системы распознавания лиц становятся лучше, они все еще не оправдали ожиданий. Требуется лучший алгоритм определения местоположения лица. Во многих случаях существующее программное обеспечение либо вообще не может обнаружить лицо, либо находит «лицо» в неправильном месте. Это ухудшает результат. Кроме того, алгоритмы испытывают трудности с различением очень похожих людей, таких как близнецы, и повторная регистрация необходима для каждого существенного изменения прически или бороды. Очки еще больше усложняют ситуацию. Можно обмануть с помощью фотографии. Имитация лица обеспечивает основу определения живости в большинстве случаев. Требуется, чтобы пользователь ухмыльнулся или моргнул.

Геометрия сетчатки: самая существенная проблема со сканированием сетчатки заключается в его инвазивности. Сканирование сетчатки требует инвазивной процедуры, которую должны пройти самостоятельно. Необходимо направлять лазерный луч через роговицу или край. Сканеры сетчатки также не просты в использовании. Сканируемый человек должен следовать инструкциям оператора, что требует специальных знаний. С другой стороны, устройства для сканирования сетчатки предположительно точны и

используются в ситуациях, требующих высокого уровня безопасности.

Метод распознавания голоса: наибольшее преимущество систем проверки говорящего, согласно методике распознавания говорящего (голоса), заключается в том, что они не требуют специального и дорогостоящего оборудования. Можно использовать его на расстоянии, используя свой телефон. Фоновый шум является серьезной проблемой, которая снижает точность, хотя высокая частота дискретизации не является необходимой. Поскольку он опирается на поведенческие черты, на него может неблагоприятно влиять текущее физическое и эмоциональное состояние человека.

Метод проверки подписи: подписи двух людей никогда не бывают абсолютно одинаковыми, поскольку это так, в данных, собранных с подписи человека, должно быть некоторое пространство для маневра. Что касается систем динамики подписи, большинство в первую очередь проверяют динамику. Результирующая подпись полностью игнорируется ими. Небольшое количество систем утверждает, что они могут проверять не только динамику подписи, но и окончательный вид подписи. Из того, что мы видели, приемлемая подпись может выглядеть совсем иначе, чем основной шаблон, если система не проверяет результирующую динамику по сравнению с подписью. Поскольку лица, принимающие решения, обычно отдают предпочтение быстрому написанию, теоретически возможно успешно подделать подпись, даже если результирующая подпись заметно отличается.

Размер данных, полученных во время процедуры подписания, составляет около 20 КБ.

Размер основного шаблона может варьироваться от нескольких килобайт до, примерно, 90 байт, в зависимости от количества используемых подписей.

Распознавание подписи испытывает трудности с распознаванием совпадений, когда размер основного шаблона довольно большой, что делает его непригодным для чего-либо, кроме проверки.

Хотя производители заявляют о коэффициенте кроссовера около 2 % для биометрических устройств с динамикой подписи, наш собственный опыт показал, что этот показатель намного ниже.

В таблице 1 представлен анализ результатов оценки.

Таблица 1 – Оценка биометрических методов

Биометрический объект	Процент ошибок	Количество точек идентификации	Комментарии
Лицо	10 %	37437	Разнообразный свет, в помещении
Отпечаток пальца	2 %	2500	Вращение и преувеличенное искажение при идентификации
Геометрия руки	1 %	129	С кольцами и средствами защиты высокий процент ошибок
Зрачок	0,99 %	1224	Внутренняя среда
Подпись	0,1 %	15	В течение 6 месяцев постоянна, потом может измениться
Голос	10 %	30	Текстозависимый и многоязычный

Поскольку технология биометрической аутентификации только недавно начала использоваться в коммерческих целях в общественной сфере, она считается новой технологической разработкой.

Биометрическая технология имеет несколько применений, одно из которых – в системах безопасности. Она предлагает точные ответы на вопросы с идентификацией и обнаружением. Повышенная безопасность, эффективная аутентификация, меньше мошенничества, простота использования и внедрения – вот лишь некоторые из ее многочисленных положительных аспектов, которые могут улучшить человеческую жизнь.

Кроме того, нет необходимости тратить деньги на менеджера паролей или генератор токенов. Напротив, существует несколько нерешенных проблем с биометрическими системами безопасности, включая конфиденциальность данных, физическую конфиденциальность и религиозные возражения. После рассмотрения всего этого становится ясно, что все эти новые технологии, несомненно, улучшат и упростят нашу жизнь. Методы, включающие биометрическое местоположение и подготовку наборов данных, являются

неотъемлемой частью идентификации человека, что позволяет проводить исследования отдельных лиц для количественных целей.

Вывод по разделу.

В разделе определено, что наибольшей популярностью среди биометрических технологий пользуется технология идентификации при помощи отпечатка пальца или руки, но при массовом сканировании необходимо прикасаться к поверхностям, которые могут быть загрязнены или заражены.

Определено, что для сканирования сетчатки глаза человеку необходимо снять очки, поднести глаз к сканеру, сфокусироваться на фиксированной точке и оставаться неподвижными в течение 10-15 секунд, что также в условиях массовой идентификации займёт большое количество времени.

Преимуществом технологии идентификации персонала по сосудистым рисункам руки является быстрота и отсутствие необходимости прикасаться к поверхностям сканеров.

Сканирование лица требует от работников снимать средства защиты (очки, маски, респираторы, каски, что в условиях химического производства может быть не безопасным.

Распознавание динамических подписей применима в основном для идентификации офисного персонала.

Технология распознавания голоса не применима в условиях повышенного шума на производстве.

3 Совершенствование контроля доступа в организации

На территории и зданиях ООО «Тольяттикаучук» существуют производства, на которые в целях обеспечения безопасности персонала и производства в целом необходимо установить внутренний контроль доступа, например, в отделение получения щавелевой кислоты.

Технологический процесс получения щавелевой кислоты характеризуется наличием токсичных жидких и газообразных продуктов, оказывающих вредное действие на организм человека.

Наименование сырья, полупродуктов, готовой продукции (вещества, % масс.), отходов производства, их характеристика токсичности (воздействия на организм человека) и ПДК в воздухе рабочей зоны представлены в таблице 2.

Таблица 2 – Характеристика токсичности (воздействия на организм человека) и ПДК сырья, полупродуктов, готовой продукции в воздухе рабочей зоны

Наименование сырья, полупродуктов, готовой продукции, отходов производства	Класс опасности	Температура, °С			ПДК в воздухе рабочей зоны	Характеристика токсичности (воздействия на организм человека)
		кипения	плавления	самовоспламенения		
Кислота азотная	3	83	минус 42	–	2	Вещество оказывает разъедающее действие на глаза, кожу и дыхательные пути. Разъедающее действие при проглатывании в том числе. Вдыхание паров может вызвать отек легких
Кислота серная	2	337	10	–	1	Очень едкое вещество, поражающее все ткани организма. При вдыхании паров этих веществ они вызывают затруднение дыхания, кашель, нередко ларингит, трахеит, бронхит и т. д. Попадание кислоты на глаза в высокой концентрации может привести к полной потере зрения.

Продолжение таблицы 2

Наименование сырья, полупродуктов, готовой продукции (вещества, % масс.), отходов производства	Класс опасности	Температура, °С			ПДК в воздухе рабочей зоны	Характеристика токсичности (воздействия на организм человека)
		кипения	плавления	самовоспламенения		
Кислота щавелевая	2	–	365	518	1	Может быть опасной в случае вдыхания; опасна и чрезвычайно разрушительна по отношению к биологическим тканям слизистых оболочек и верхних дыхательных путей. Опасна в случае проглатывания в чистом виде; может вызывать химические ожоги при контакте с кожей или попадании в глаза в больших количествах. Симптомы включают чувство жжения, кашель, хрипы, ларингит, одышку, спазм, воспаление и отёк гортани, воспаление и отёк бронхов, пневмонит, отёк легких
Оксид азота (II)	3	минус 152	минус 164	–	5	Вещество раздражает глаза и дыхательные пути. Вдыхание этого вещества может вызвать отек легких. Вещество может оказывать действие на кровь, приводя к образованию метгемоглобина. Воздействие может вызвать смерть. Эффекты могут быть отсроченными
Оксид азота (IV)	3	21.1	минус 11.2	–	2	Вещество раздражает глаза, кожу и дыхательные пути. Вдыхание газа или пара может вызвать отек легких. Воздействие на высоком уровне может вызвать смерть. Эффекты могут быть отсроченными. Реагирует с водой с образованием азотной кислоты и оксида азота.

Товарная форма щавелевой кислоты для установки И-6 производства

изопрена – в виде водного раствора с концентрацией до 15 % масс.

Как следует из таблицы 2, технологический процесс получения щавелевой кислоты характеризуется наличием токсичных жидких и газообразных продуктов, оказывающих вредное действие на организм человека. Соответственно, допуск в помещения с наличием токсичных жидких и газообразных продуктов только обученных работников правилам безопасности при нахождении в данных помещениях отделения позволит снизить количество несчастных случаев, производственного травматизма и заболеваний персонала ООО «Тольяттикаучук».

Отделение получения щавелевой кислоты состоит из следующих узлов:

- узел синтеза, кристаллизации, отжим кристаллизации;
- узел перекристаллизации, сбор конденсата, узел аварийных сбросов;
- узел нейтрализации химических стоков, регенерация маточного раствора;
- узел поглощения нитрозных газов;
- узел снабжения энергоресурсами.

Для защиты оборудования от завышения давления предусмотрены и установлены предохранительные клапаны, сброс от которых производится в емкость Е-6. Для обеспечения безаварийной работы насосы Н-3/1,2; Н-1/1А,Б; Н-1/2А,Б; Н-7/1,2; Н-5/1,2; Н-6; Н-4/1,2; Н-2/1,2; Н-8/1,2, Н-11/1,2, Н-12 – оснащены блокировками, предусмотрена световая и звуковая сигнализация останова электродвигателей насосов.

Азотная кислота с концентрацией не менее 57 % мас. поступает на установку из цеха складского хозяйства в еврокубах. Еврокуб подсоединяется по временной линии к дозировочному насосу Н-9, и далее азотная кислота подается:

- в емкость Е-3 для приготовления маточного раствора;
- в реактор Р-1, Р-2 для проведения основной реакции синтеза щавелевой кислоты.

Давление в линии подачи азотной кислоты регистрируется КИПиА.

Расход подачи азотной кислоты регистрируется КИПиА и выдерживается регулированием вращения частоты электродвигателя КИПиА. При откачке заданного объема азотной кислоты электродвигатель насоса отключается.

На линии подачи азотной кислоты установлены отсечные клапаны: в емкость Е-3; в реактор Р-1; в реактор Р-2.

Серная кислота с концентрацией 92,5-94,0 % мас. поступает на установку из цеха складского хозяйства в еврокубах. Еврокуб подсоединяется по временной линии к дозировочному насосу Н-10, и далее серная кислота подается в емкость Е-3 для приготовления маточного раствора. Давление в линии подачи серной кислоты регистрируется КИПиА.

Расход подачи азотной кислоты регистрируется КИПиА и выдерживается регулированием вращения частоты электродвигателя КИПиА. При откачке заданного объема серной кислоты электродвигатель насоса Н-10 отключается.

Щавелевая кислота, полученная в процессе синтеза, выделяется кристаллизацией, путем охлаждения реакционной массы при перемешивании в кристаллизаторе. Из кристаллизатора суспензия поступает на фильтрующую центрифугу. На центрифуге происходит отделение и промывка кристаллов щавелевой кислоты. Маточный раствор из центрифуги поступает в сборник, откуда насосом подается на орошение скрубберов.

После отделения кристаллов, через фильтр, щавелевая кислота направляется на узел перекристаллизации, производится отмывка щавелевой кислоты от примесей. Отмывка осуществляется путем растворения кристаллов в воде и охлаждением полученного раствора, с последующим повторным отделением и промывкой кристаллов на центрифуге.

Проанализировав технологию получения щавелевой кислоты предлагается систему контроля и управления доступом (далее – СКУД) с использованием биометрии установить при входе в здание складского хозяйства и в помещения, где установлены линии подачи серной и азотной

кислоты, а также реакторы Р-1, Р-2 и ёмкость маточного раствора.

Определение и аутентификация могут осуществляться несколькими методами, такими как отпечатки пальцев, сканирование вен рук, подпись, лицо, сканирование глаз, голос.

Выбор способа биометрической идентификации обусловлен:

- ношением касок, очков и других средств защиты лица (для сканирования черт лица не подходит);
- высокого уровня шума в помещениях предприятия (для сканирования голоса не подходит);
- гигиеническими требованиями (для сканирования отпечатка пальцев не подходит).

Для установки биометрического СКУД при входе в здание складского хозяйства и в помещения, где установлены линии подачи серной и азотной кислоты, а также реакторы Р-1, Р-2 и ёмкость маточного раствора в связи с тем, что работники постоянно носят СИЗ (перчатки, респираторы, очки, каски) подходит только технология сканирования вен рук (рисунок 2).

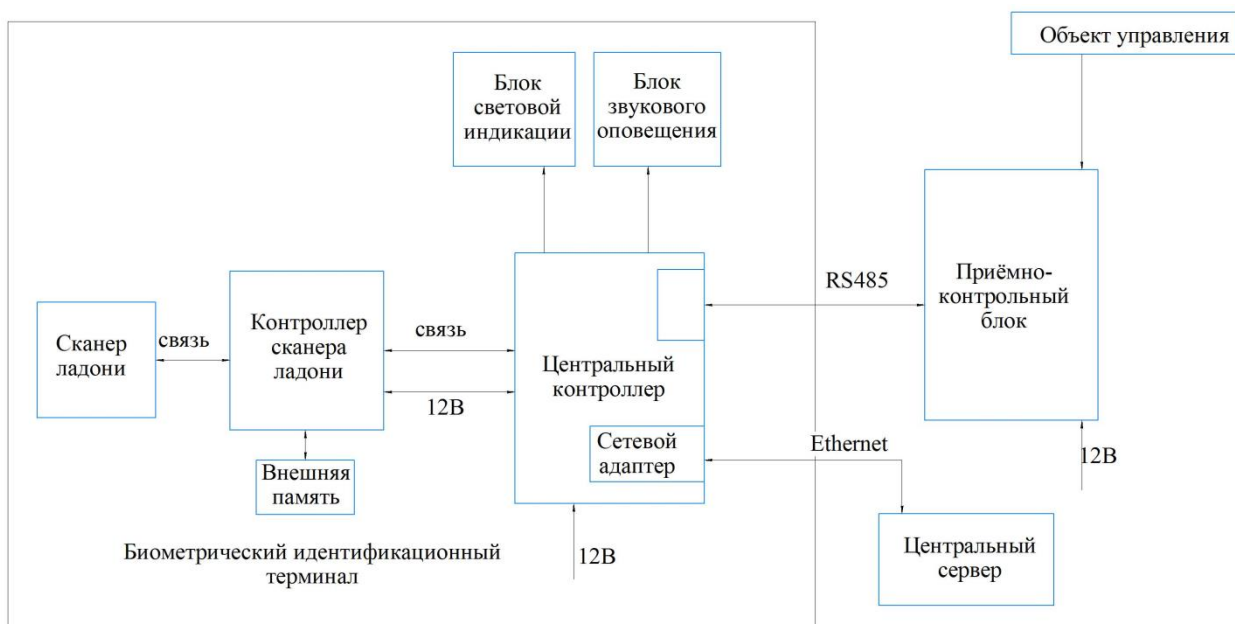


Рисунок 2 – Предлагаемая схема биометрической СКУД

Возможны как контактные, так и бесконтактные типы оборудования для визуализации сосудов. Преимущество бесконтактного метода заключается в том, что человеку, предоставляющему биометрические данные, даже не нужно прикасаться к датчику.

В качестве сканера ладони выбран считыватель BioSmart PalmJet, который изображен на рисунке 3.



Рисунок 3 – Считыватель BioSmart PalmJet [1]

Характеристика:

- тип биометрического сканера – оптический, инфракрасный;
- типы поддерживаемых карт – Mifare;
- расстояние ладони от сканера, см – от 4 до 9;
- наличие встроенного считывателя RFID-меток – да;
- вероятность ошибочного предоставления доступа по биометрическим данным, FAR – 10^{-5} - 10^{-8} .

Выводы по разделу.

В разделе определено, что на опасном производственном объекте

ООО «Тольяттикаучук» отсутствует автоматизированный СКУД для работников, которые не работают в помещениях данных объектов, а доступ работников осуществляется при помощи вызывной панели и радиобрелков. Из-за того, что часто работники забывают брелки, доступ производится по вызывной панели.

Допуск в помещения с наличием токсичных жидких и газообразных продуктов только работников, обученных правилам безопасности, при нахождении в данных помещениях отделения позволит снизить количество несчастных случаев, производственного травматизма и заболеваний персонала ООО «Тольяттикаучук».

Для установки биометрического СКУД при входе в здание складского хозяйства и в помещения, где установлены линии подачи серной и азотной кислоты, а также реакторы Р-1, Р-2 и ёмкость маточного раствора в связи с тем, что работники постоянно носят СИЗ (перчатки, респираторы, очки, каски) предложена технология сканирования вен рук.

Разработана схема биометрической СКУД с использованием скана вен ладони руки.

4 Охрана труда

В соответствии с Приказом Минтруда России от 29.10.2021 № 776н «Об утверждении Примерного положения о системе управления охраной труда» [13] произведём оценку профессиональных рисков [14] для рабочих мест. Характеристика рабочих мест представлена в таблице 3.

Таблица 3 – Характеристика рабочих мест

Наименование рабочего места	Оборудование, инструмент на рабочем месте	Материалы, вещества	Виды выполняемых работ, трудовых операций
Инженер	Технологические установки и оборудование	Технологические вещества и материалы	Проведение работ по наладке и контролю технологических процессов
Лаборант	Оборудование лаборатории,	Кислоты, щёлочи	Лабораторные исследования веществ, материалов
Электромеханик	Электрическое оборудование, щиты подключения технологического оборудования	Технологические вещества и материалы	Ремонт и обслуживание электрического оборудования

Реестр рисков на рабочем месте инженера представлен в таблице 4.

Таблица 4 – Реестр рисков на рабочем месте инженера

Опасность	ID	Опасное событие
9. Вредные химические вещества в воздухе рабочей зоны	9.1	Отравление воздушными взвешями вредных химических веществ в воздухе рабочей зоны
12. Аэрозоли преимущественно фиброгенного действия (АПФД)	12.3	Повреждение органов дыхания вследствие воздействия воздушных взвесей вредных химических веществ
24. Монотонность труда при выполнении однообразных действий или непрерывной и устойчивой концентрации внимания в условиях дефицита сенсорных нагрузок	24.1.	Психоэмоциональные перегрузки
24. Диспетчеризация процессов, связанная с длительной концентрацией внимания	24.4.	Психоэмоциональные перегрузки

Реестр рисков на рабочем месте лаборанта представлен в таблице 5.

Таблица 5 – Реестр рисков на рабочем месте лаборанта

Опасность	ID	Опасное событие
9. Вредные химические вещества в воздухе рабочей зоны	9.1	Отравление воздушными взвешьями вредных химических веществ в воздухе рабочей зоны
12. Аэрозоли преимущественно фиброгенного действия (АПФД)	12.3	Повреждение органов дыхания вследствие воздействия воздушных взвесей вредных химических веществ
23. Физические перегрузки при чрезмерных физических усилиях при подъеме предметов и деталей, при перемещении предметов и деталей	23.1.	Повреждение костно-мышечного аппарата работника при физических перегрузках
27. Электрический ток	27.1	Контакт с частями электрооборудования, находящимися под напряжением

Реестр рисков на рабочем месте электромеханика представлен в таблице 6.

Таблица 6 – Реестр рисков на рабочем месте электромеханика

Опасность	ID	Опасное событие
9. Вредные химические вещества в воздухе рабочей зоны	9.1	Отравление воздушными взвешьями вредных химических веществ в воздухе рабочей зоны
12. Аэрозоли преимущественно фиброгенного действия (АПФД)	12.3	Повреждение органов дыхания вследствие воздействия воздушных взвесей вредных химических веществ
27. Электрический ток	27.1	Контакт с частями электрооборудования, находящимися под напряжением
	27.2	Отсутствие заземления или неисправность электрооборудования
	27.3	Нарушение правил эксплуатации и ремонта электрооборудования, неприменение СИЗ
	27.4	Воздействие электрической дуги
27. Шаговое напряжение	27.5	Поражение электрическим током

Анкета уровня профессиональных рисков на рабочем месте инженера отражена в таблице 7.

Таблица 7 – Анкета уровня рисков на рабочем месте инженера

Рабочее место	Опасность	Опасное событие	Степень вероятности, А	Коэффициент, А	Тяжесть последствий, U	Коэффициент, U	Оценка риска, R	Значимость оценки риска
Инженер	9	9.1	Вероятно	4	Значительная	3	12	Средний
	12	12.3	Вероятно	4	Значительная	3	12	Средний
	24	24.1	Возможно	3	Значительная	3	9	Средний
		24.4	Возможно	3	Значительная	3	9	Средний

Анкета профессиональных рисков лаборанта представлена в таблице 8.

Таблица 8 – Анкета профессиональных рисков на рабочем месте лаборанта

Рабочее место	Опасность	Опасное событие	Степень вероятности, А	Коэффициент, А	Тяжесть последствий, U	Коэффициент, U	Оценка риска, R	Значимость оценки риска
Лаборант	9	9.1	Вероятно	4	Значительная	3	12	Средний
	12	12.3	Вероятно	4	Значительная	3	12	Средний
	23	23.1.	Возможно	3	Незначительная	2	6	Низкий
	27	27.1	Вероятно	4	Значительная	3	12	Средний

Анкета уровня рисков электромеханика отражена в таблице 9.

Таблица 9 – Анкета уровня профессиональных рисков электромеханика

Рабочее место	Опасность	Опасное событие	Степень вероятности, А	Коэффициент, А	Тяжесть последствий, U	Коэффициент, U	Оценка риска, R	Значимость оценки риска
Электромеханик	9	9.1	Вероятно	4	Значительная	3	12	Средний
	12	12.3	Вероятно	4	Значительная	3	12	Средний

Продолжение таблицы 9

Рабочее место	Опасность	Опасное событие	Степень вероятности, А	Коэффициент, А	Тяжесть последствий, U	Коэффициент, U	Оценка риска, R	Значимость оценки риска
Электромеханик	27	27.1	Вероятно	4	Катастрофическая	5	20	Высокий
		27.2	Вероятно	4	Крупная	4	16	Средний
		27.3	Вероятно	4	Катастрофическая	5	20	Высокий
		27.4	Вероятно	4	Катастрофическая	5	20	Высокий
		27.5	Вероятно	4	Крупная	4	16	Средний

Количественная оценка риска рассчитывается по формуле 1:

$$R=A \cdot U, \quad (1)$$

где А – коэффициент вероятности;

U – коэффициент тяжести последствий.

Оценка вероятности представлена в таблице 10.

Таблица 10 – Оценка вероятности

Степень вероятности		Характеристика	Коэффициент, А
1	Весьма маловероятно	Практически исключено. Зависит от следования инструкции. Нужны многочисленные поломки/отказы/ошибки.	1
2	Маловероятно	Сложно представить, однако может произойти. Зависит от следования инструкции. Нужны многочисленные поломки/отказы/ошибки.	2
3	Возможно	Иногда может произойти. Зависит от обучения (квалификации). Одна ошибка может стать причиной аварии/инцидента/несчастного случая.	3

Продолжение таблицы 10

Степень вероятности		Характеристика	Коэффициент, А
4	Вероятно	Зависит от случая, высокая степень возможности реализации. Часто слышим о подобных фактах. Периодически наблюдаемое событие.	4
5	Весьма вероятно	Обязательно произойдет. Практически несомненно. Регулярно наблюдаемое событие.	5

Оценка степени тяжести последствий представлена в таблице 11.

Таблица 11 – Оценка степени тяжести последствий

Тяжесть последствий		Потенциальные последствия для людей	Коэффициент, U
5	Катастрофическая	Групповой несчастный случай на производстве (число пострадавших 2 и более человек). Несчастный случай на производстве со смертельным исходом. Авария. Пожар.	5
4	Крупная	Тяжелый несчастный случай на производстве (временная нетрудоспособность более 60 дней). Профессиональное заболевание. Инцидент.	4
3	Значительная	Серьезная травма, болезнь и расстройство здоровья с временной утратой трудоспособности продолжительностью до 60 дней. Инцидент.	3
2	Незначительная	Незначительная травма – микротравма (легкие повреждения, ушибы), оказана первая медицинская помощь. Инцидент. Быстро потушенное загорание.	2
1	Приемлемая	Без травмы или заболевания. Незначительный, быстроустраняемый ущерб.	1

Оценка риска, R:

- 1-8 (низкий);
- 9-17 (средний);
- 18-25 (высокий).

Контроль и управление технологическим процессом технологический персонал ведет в автоматизированной системе управления технологическим процессом (далее – АСУТП). Эти значения выводятся в АСОДУ, MES.

Безопасность производственного процесса достигается упреждением аварийных ситуаций, и в течение всего срока эксплуатации технологического оборудования должна быть обеспечена соблюдением следующих мероприятий:

- соблюдением регламентов режима работы и обслуживания производственного оборудования;
- использованием сертифицированных исходных материалов, не оказывающих опасного и/или вредного воздействия на эксплуатирующий персонал;
- применением производственного оборудования, не являющегося источником травматизма и профессиональных заболеваний;
- применением надежно действующих и регулярно проверяемых контрольно-измерительных приборов, устройств противоаварийной защиты, средств получения, переработки и передачи информации;
- рациональным размещением производственного оборудования и организацией рабочих мест;
- профессиональным отбором, обучением работающих, проверкой их знаний и навыков безопасности труда в соответствии с требованиями;
- применением средств защиты работающих, соответствующих характеру проявления возможных опасных и вредных производственных факторов;
- осуществлением технических и организационных мер по предотвращению пожара и противопожарной защите по ГОСТ 12.1.004-91 [19];
- соответствующим обозначением опасных зон производства работ;
- включением требований безопасности в нормативно-техническую, проектно-конструкторскую и технологическую документацию, соблюдением этих требований, а также требований

соответствующих правил безопасности и других документов по охране труда;

- соблюдением установленного порядка проведения и организации работ, высокой производственной, технологической и трудовой дисциплины.

Для обеспечения безопасности предусматриваются следующие меры:

- устранение непосредственного контакта работающих с опасными веществами;
- организация технологического процесса, при котором опасные и вредные производственные факторы, не превышают предельно допустимых уровней концентраций;
- применение средств защиты работающих;
- использование сигнальных цветов и знаков безопасности.

Безопасность труда при эксплуатации электроустановок предлагается обеспечивать следующими решениями:

- выбор схемы электроснабжения потребителей электроэнергии отвечает требованиям их надежной и устойчивой работы;
- объекты, для обслуживания которых требуется подъем рабочего на высоту 0,75 м и более, оборудуются лестницами шириной 0,70 м с перилами;
- перильное ограждение переходных мостиков и площадок обслуживания по технике безопасности предусмотрено высотой 1250 мм с продольными планками, расположенными на расстоянии не более 40 см друг от друга, и бортиком высотой не менее 15 см.

Вывод по разделу.

В разделе определено, что по результатам оценки рисков «высокий» риск выявлен на рабочем месте электромеханика в связи с опасностью воздействия электрического тока. Разработаны мероприятия по снижению всех идентифицированных рисков.

5 Охрана окружающей среды и экологическая безопасность

Оценка антропогенной нагрузки ООО «Тольяттикаучук» на окружающую среду представлена в таблице 12

Таблица 12 – Антропогенная нагрузка ООО «Тольяттикаучук» на окружающую среду

Наименование объекта	Подразделение	Воздействие на атмосферный воздух	Воздействие на водные объекты	Отходы (перечислить виды отходов)
ООО «Тольяттикаучук»	Производство щавелевой кислоты	Газообразные	Ливневые стоки	ТКО
Количество в год		0,735788 т	250000 м ³	45,82 т

Загрязнение окружающей среды будет минимальным при выдерживании заданных норм технологического режима на всех стадиях производства щавелевой кислоты, содержании в исправном состоянии технологического оборудования:

- трубопроводов;
- запорных, предохранительных;
- регулирующих устройств.

Определим, соответствуют ли технологии наилучшим доступным. Результаты анализа технологии на производстве представлены в таблице 13.

Таблица 13 – Результаты соответствия технологий на производстве

Структурное подразделение		Наименование технологии	Соответствие наилучшей доступной технологии
номер	наименование		
1	Производство щавелевой кислоты	Обращение с отходами	Соответствует

Перечень загрязняющих веществ, включенных в план-график контроля стационарных источников выбросов [11] представлен в таблице 14.

Таблица 14 – Перечень загрязняющих веществ

Номер	Наименование загрязняющего вещества
1	Метан
2	Пентан
3	Амилены
4	Пиперилен
5	ЦПД
6	Изопрен
7	Метанол
8	Амиловый спирт
9	Гексан
10	ДМЭ
11	МТАЭ
12	МПЭ

Производственный контроль в области обращения с отходами, осуществляется лицами, ответственными за обращение с отходами и/или осуществляющими контроль в указанной области, имеющими свидетельства на право обращения с опасными отходами в соответствии с Федеральным законом РФ №89-ФЗ [10].

При обслуживании оборудования и трубопроводов особое внимание должно быть обращено на осуществление контроля:

- за герметичностью оборудования и арматуры;
- за плотностью фланцевых соединений;
- за толщиной стенок трубопроводов неразрушающим методом с периодичностью, определенной нормами и заводом-изготовителем.

Результаты контроля стационарных источников выбросов загрязняющих веществ в атмосферный воздух представлены в таблице 15.

Результаты проведения проверок работы очистных сооружений, включая результаты технологического контроля эффективности работы очистных сооружений на всех этапах и стадиях очистки сточных вод и обработки осадков [16] представлены в таблице 16.

Сведения об образовании, утилизации, обезвреживании, размещении отходов производства и потребления представлены в таблице 17.

Таблица 15 – Результаты контроля стационарных источников выбросов загрязняющих веществ в атмосферный воздух

Номер источника	Структурное подразделение (площадка, цех или другое)		Источник		Наименование загрязняющего вещества	Предельно допустимый выброс или временно согласованный выброс, г/с	Фактический выброс, г/с	Превышение предельно допустимого выброса или временно согласованного выброса в раз (гр. 8/гр. 7)	Дата отбора проб	Общее количество случаев превышения предельно допустимого выброса или временно согласованного выброса	Примечание
	номер	наименование	номер	наименование							
1	1	Производство щавелевой кислоты	01	Наружная установка	Метан	0,029305	0,029305	-	20.01.2024	-	-
					Пентан	0,434743	0,434743	-	20.01.2024	-	-
					Амилены	0,058655	0,058655	-	20.01.2024	-	-
					Пипериле	0,000980	0,000980	-	20.01.2024	-	-
					н						
					ЦПД	0,000095	0,000095	-	20.01.2024	-	-
					Изопрен	0,004058	0,004058	-	20.01.2024	-	-
					Метанол	0,176435	0,176435	-	20.01.2024	-	-
					Амиловый спирт	0,000020	0,000020	-	20.01.2024	-	-
					Гексан	0,000052	0,000052	-	20.01.2024	-	-
					ДМЭ	0,000756	0,000756	-	20.01.2024	-	-
					МТАЭ	0,026697	0,026697	-	20.01.2024	-	-
					МПЭ	0,004012	0,004012		20.01.2024	-	-

Таблица 16 – Результаты проведения проверок работы очистных сооружений, включая результаты технологического контроля эффективности работы очистных сооружений на всех этапах и стадиях очистки сточных вод и обработки осадков

Тип очистного сооружения	Год ввода в эксплуатацию	Сведения о стадиях очистки, с указанием сооружений очистки сточных вод, в том числе дренажных, вод, относящихся к каждой стадии	Объем сброса сточных, в том числе дренажных, вод, тыс. м ³ /сут.; тыс. м ³ /год			Наименование загрязняющего вещества или микроорганизма	Дата контроля (дата отбора проб)	Содержание загрязняющих веществ, мг/дм ³			Эффективность очистки сточных вод, %	
			проектный	допустимый, в соответствии с разрешительным документом на право пользования водным объектом	фактический			проектное	допустимое, в соответствии и с разрешением на сброс веществ и микроорганизмов в водные объекты	фактическое	проектная	фактическая
Очистные сооружения БИО	2010	Усреднитель объемом 500 м ³ . Резервуар очистки вод объемом 500 м ³ . Участок обеззараживания	1200; 438	1500; 500	600; 250	Нефтепродукты	22.02.2023	0,5	0,2	0,1	-	95

Таблица 17 – Сведения об образовании, утилизации, обезвреживании, размещении отходов производства и потребления

N строки	Наименование видов отходов	Код по федеральному классификацио нному каталогу отходов, далее - ФККО	Класс опасности отходов	Наличие отходов на начало года, тонн		Образов ано отходов, тонн	Получено отходов от других индивидуальных предпринимателе й и юридических лиц, тонн	Утилизир овано отходов, тонн	Обезврежен о отходов, тонн
				хранени е	накоплени е				
1	2	3	4	5	6	7	8	9	10
1	«Лампы ртутные, ртутно-кварцевые, люминесцентные, утратившие потребительские свойства)» [15]	4 71 101 01 52 1	1	0	0	0,020	0	0,020	0
2	«Мусор от офисных и бытовых помещений организаций несортированный (исключая крупногабаритный)» [15]	7 33 100 01 72 4	4	0	0	5,30	0	15,30	0
3	«Отходы, содержащие незагрязненные черные металлы (в том числе чугунную и/или стальную пыль), несортированные» [15]	4 61 010 03 20 4	4	0	0	17,50	0	17,50	0

Продолжение таблицы 17

N строки	Наименование видов отходов	Код по федеральном у классификац ионному каталогу отходов, далее - ФККО	Класс опасност и отходов	Наличие отходов на начало года, тонн		Образо вано отходо в, тонн	Получено отходов от других индивидуальн ых предпринимат елей и юридических лиц, тонн	Утилизи ровано отходов, тонн	Обезврежен о отходов, тонн
				хранен ие	накоплен ие				
1	2	3	4	5	6	7	8	9	10
5	«Смет с территории предприятия малоопасный » [15]	7 33 390 01 71 4	4	0	0	23,00	0	23,00	0
всего		для обработки	для утилизации		для обезвреживания		для хранения		для захоронения
11		12	13		14		15		16
0,020		-	-		-		-		0,020
5,30		-	-		-		-		5,30
17,50		-	-		-		-		17,50
3,5		-	-		-		-		23,00

Продолжение таблицы 17

Размещено отходов на эксплуатируемых объектах, тонн					Наличие отходов на конец года, тонн	
всего	хранение на собственных объектах размещения отходов, далее - ОРО	захоронение на собственных ОРО	хранение на сторонних ОРО	захоронение на сторонних ОРО	хранение	накопление
16	17	18	19	20	21	22
0,020	0	0	0	0,020	0	0
5,30	0	0	0	5,30	0	0
17,50	0	0	0	17,50	0	0
23,00	0	0	0	23,00	0	0

Для исключения разгерметизации оборудования и предупреждения аварийных выбросов опасных веществ при эксплуатации требуется соблюдать следующие правила:

- ведение технологического процесса осуществлять в строгом соответствии с требованиями технологического регламента;
- своевременно осуществлять техническое обслуживание и ремонт аппаратов, оборудования, трубопроводов и арматуры;
- своевременно осуществлять плановый ремонт и комплексную диагностику аппаратов, оборудования, трубопроводов и арматуры;
- к обслуживанию объекта допускать лица, ознакомленные с конструкцией, принципом действия и порядком работы объекта в целом.

Накопление отходов осуществляется в герметичных контейнерах (емкостях) с крышками для защиты от воздействия атмосферных осадков, ветра и предотвращения попадания загрязняющих веществ в почву, поверхностные и подземные воды. Они оснащены надписями о виде накапливаемых отходов, его классе опасности, принадлежности контейнера (емкости), ответственного лица.

Вывод по разделу.

В разделе определено, что загрязнение окружающей среды будет минимальным при выдерживании заданных норм технологического режима на всех стадиях производства щавелевой кислоты, содержании в исправном состоянии технологического оборудования.

Основными целями деятельности объекта исследования в области обращения с отходами являются предотвращение вредного воздействия отходов производства и потребления, образующихся в процессе производственной деятельности на здоровье человека и окружающую природную среду.

6 Защита в чрезвычайных и аварийных ситуациях

Основными причинами возникновения аварийных ситуаций на объектах различного назначения являются нарушения технологических процессов на промышленных предприятиях, технические ошибки обслуживающего персонала, брак и нарушения противопожарных правил и правил техники безопасности. Степень риска возникновения аварийной ситуации зависит как от природных, так и от техногенных факторов. Естественные факторы, представляющие угрозу для осваиваемого района, характеризуются очень низкими уровнями вероятностями развития аварии.

На исследуемых сооружениях присутствуют взрывопожароопасные вещества, сооружения установки и транспортируемые продукты представляют определенную материальную ценность, на исследуемом объекте присутствует обслуживающий персонал.

Возможными причинами взрыва и пожара могут быть:

- применение открытого огня в местах, не предусмотренных для этой цели;
- разряды статического электричества, молнии;
- перегрев подшипников и других трущихся частей в насосном оборудовании, вентиляционных установках и других механизмах с вращающимися частями;
- работа двигателей техники во взрывоопасной зоне;
- эксплуатация неисправного электрооборудования;
- эксплуатация во взрывоопасной зоне электроосвещения и электрооборудования без соответствующего класса и категории взрывозащищенного исполнения;
- использование при проведении ремонтных работ искродающих инструментов;
- курение в не установленном месте;
- самовозгорание промасленных обтирочных материалов;

- совмещение проведения огневых и газоопасных работ;
- разлив углеводородов вследствие разгерметизации оборудования.

Прогнозируемые инциденты в работе и способы их устранения представлены в таблице 18.

Таблица 18 – Прогнозируемые инциденты в работе и способы их устранения

Инциденты	Возможные причины возникновения инцидентов	Действия персонала и способ устранения инцидентов
Завышение температуры низа реактора Р-1, Р-2	1. Неисправность КИПиА регистрирующих температуру низа реактора.	1. Освободить реактор в кристаллизатор К-2. Подать заявку на устранение неисправности.
	2. Неисправность РК КИПиА поз. TV 0028В, TV 0035В на линии обратного захоложенного рассола от змеевика реактора Р-1, Р-2.	1. Освободить реактор в кристаллизатор К-2. Произвести замену РК.
	3. Воздушные пробки в змеевике охлаждения рассолом.	1. Стравить воздушные пробки в верхней точке обратного рассола от змеевика реактора Р-1, Р-2 через дренаж.
Увеличилась токовая нагрузка на электродвигатель мешалки кристаллизатора	1. Большой осадок щавелевой кислоты.	1. Остановить перемещающее устройство К-1, К-2. 2. Подать воздух технологический для барботажа. 3. Поэтапно освободить кристаллизатор К-1
Уменьшилась токовая нагрузка на электродвигатель мешалки реактора	1. Механическая неисправность перемещающего устройства.	1. Остановить перемещающее устройство. 2. Освободить реактор в кристаллизатор К-1. 2. Вывести ректор в ремонт.
Сильная вибрация реактора Р-1, Р-2, кристаллизатора К-1, К-2	1. Попадание посторонних предметов между лопастями перемещающего устройства и стаканом стабилизатора. 2. Неисправен подшипник втулки скольжения стакана стабилизатора.	1. Остановить перемещающее устройство. 2. Вывести оборудование в ремонт.
Занижен показатель рН стоков, сбрасываемых в ХЗК-199	1. Неисправность КИПиА контролируемый рН среды поз. АЕ-0001	1. Сдозировать раствор щелочи в емкость Е-4 до доведения до норм 6,5-8,5 ед. рН 2. Перед откачкой емкости Е-4 в ХЗК-199 подать заявку в лабораторию ЦЗЛ ЛК С и ГП для проведения анализа сточных вод в емкости Е-4

Перечень технических средств, обеспечивающих взрывобезопасность процесса:

- блокировка и сигнализация противоаварийной защиты (ПАЗ), согласно «Ведение технологического процесса. Действия персонала при срабатывании сигнализации и блокировок»;
- сигнализаторы довзрывных концентраций, обеспечивающие контроль за состоянием воздушной среды;
- аварийные приточно-вытяжные вентиляционные системы АВ-1, АП-1 в отделениях, сблокированные с сигнализаторами довзрывных концентраций;
- приточные вентиляционные системы, обеспечивающие подпор воздуха в производственные помещения;
- предохранительные клапаны, установленные на аппаратах.

Выезд транспортных средств и лиц с материальными ценностями с территории объектов по устному распоряжению, запискам и иным документам неустановленного образца запрещен.

При пожаре, аварийных ситуациях и стихийных бедствиях, пожарные и аварийные машины с расчетами, а также санитарные машины с медицинскими работниками допускаются на территорию объектов беспрепятственно с последующим информированием оперативно-производственной службы ООО «Тольяттикаучук» [17]. В остальных случаях доступ указанных транспортных средств осуществляется на общих основаниях. При выезде с территории объектов осмотр транспортных средств производится в установленном порядке [12].

Транспортное средство имеет право въезда на объекты при выполнении следующих требований:

- наличия путевого листа с указанием в нем наименования Заказчика и маршрута движения транспортного средства по объектам ООО «Тольяттикаучук»;
- наличия средств пожаротушения (наличие искрогасителей и не

менее одного огнетушителя).

Согласно специальным требованиям предусматриваются следующие средства охраны:

- указательные и предупредительные дорожные знаки перед въездом на территорию предприятия;
- по периметру объекта установлены предупредительные, ограничительные и запрещающие знаки, определяющие запретные зоны;
- выносная система принудительной остановки транспорта автозаградитель «Гарпун» Модель А-7К;
- детектор обнаружения металлических предметов марки «Garrett Super Scanner»;
- досмотровые зеркала «УД 03.4/0,6-2,0» для досмотра автотранспорта;
- электрический шлагбаум марки «BARRIER-5000» с дистанционным управлением, резервным освещением;
- портативный обнаружитель паров взрывчатых веществ ПИЛОТ-М;
- стационарная кнопка для подачи извещения о тревоге с выводом на пульт дежурной части органов внутренних дел;
- наряды ЧОП оснащаются резиновыми палками, наручниками, средствами сотовой, телефонной и радиосвязи;
- входы в административное здание предприятия оборудованы системой СКУД и турникетами;
- критически важные объекты предприятия оснащены системами видеонаблюдения;
- система звукового оповещения (громкой диспетчерской связью) по всем промплощадкам предприятия;
- система защиты периметра (интегрированная система безопасности – система охранного телевидения (видеонаблюдения), охранной

сигнализацией [7].

В соответствии с п. 4 СП 132.13330.2011 [17] антитеррористическая защищенность объекта обеспечивается посредством установления в нормативных документах эксплуатирующей организации значений параметров объекта, отвечающих установленным в законодательстве требованиям антитеррористической защищенности.

Охрана объекта осуществляется ЧОП и техническими средствами охраны. Кроме того, охрана опасных объектов осуществляется ФГУП «Охрана» Росгвардии России.

Также охрану объектов осуществляет в круглосуточном режиме мобильная группа, путём объезда и проверки всех объектов, находящихся на территории.

Паспорт безопасности представлен в Приложении А.

Вывод по разделу.

В разделе определено, что на ООО «Тольяттикаучук» специальным требованиям предусматриваются средства охраны.

При пожаре, аварийных ситуациях и стихийных бедствиях, пожарные и аварийные машины с расчетами, а также санитарные машины с медицинскими работниками допускаются на территорию объектов беспрепятственно с последующим информированием оперативно-производственной службы ООО «Тольяттикаучук». В остальных случаях доступ указанных транспортных средств осуществляется на общих основаниях. При выезде с территории объектов осмотр транспортных средств производится в установленном порядке.

На пожаро- и взрывоопасных объектах ООО «Тольяттикаучук» размещены технические средства, обеспечивающие взрывобезопасность процесса производства.

7 Оценка эффективности мероприятий по обеспечению техносферной безопасности

В работе определено, что производственные помещения, задействованные в технологическом процессе получения щавелевой кислоты, характеризуются наличием токсичных жидких и газообразных продуктов, оказывающих вредное действие на организм человека. Предлагается дополнить существующую систему контроля доступа в здания и помещения системами биометрической идентификации работников при помощи скана вен руки.

План мероприятий по обеспечению техносферной безопасности представлен в таблице 19.

Таблица 19 – План реализации мероприятий

Мероприятия	Цель мероприятий	Срок исполнения	Ответственное лицо	Стоимость, руб.	Источник финансирования
Проектирование биометрической системы контроля доступа	Снижение травматизма за счёт контроля доступа в опасные помещения	Июль 2025 г.	Проектная организация	25000	Бюджет ООО «Тольяттикаучук»
Закупка оборудования		Июль 2025 г.	Отдел снабжения	600000	Бюджет ООО «Тольяттикаучук»
Монтаж биометрической системы контроля доступа		Август 2025 г.	Организация по договору на монтаж системы	180000	Бюджет ООО «Тольяттикаучук»

Допуск в наиболее опасные производственные помещения только обученных работников правилам безопасности при нахождении в данных помещениях отделения позволит снизить количество несчастных случаев и производственного травматизма персонала ООО «Тольяттикаучук».

Рассчитаем величину скидки к страховому тарифу по обязательному социальному страхованию для ООО «Тольяттикаучук» на 2026 г.

Данные для расчетов скидок и надбавок представлены в таблице 20.

Таблица 20 – Данные для расчетов скидок и надбавок

Показатель	Условные обозначения	Единицы измерения	2022	2023	2024
«Среднесписочная численность работающих» [21]	N	чел	3500	3500	3500
«Количество страховых случаев за год» [21]	K	шт.	1	2	0
«Количество страховых случаев за год, исключая со смертельным исходом» [21]	S	шт.	1	2	0
«Число дней временной нетрудоспособности в связи со страховым случаем» [21]	T	дн.	50	75	0
«Сумма обеспечения по страхованию» [21]	O	руб.	100000	200000	0
«Фонд заработной платы за год» [21]	ФЗП	руб.	200000 0000	2000000 000	200000 0000
«Число рабочих мест, на которых проведена оценка условий труда» [21]	q ₁₁	шт	-	3500	-
«Число рабочих мест, подлежащих специальной оценке условий труда» [21]	q ₁₂	шт.	-	3500	-
«Число рабочих мест, отнесенных к вредным и опасным классам условий труда по результатам аттестации» [21]	q ₁₃	шт.	-	1200	-
«Число работников, прошедших обязательные медицинские осмотры» [21]	q ₂₁	чел.	3500	3500	3500
«Число работников, подлежащих направлению на обязательные медицинские осмотры» [21]	q ₂₂	чел.	3500	3500	3500

Рассчитаем скидку на страхование работников по формуле 2:

$$C(\%) = \left\{ 1 - \frac{\left(\frac{a_{cmp}}{a_{вэд}} + \frac{b_{cmp}}{b_{вэд}} + \frac{c_{cmp}}{c_{вэд}} \right)}{3} \right\} \cdot q_1 \cdot q_2 \cdot 100, \quad (2)$$

Показатель $a_{стр}$ рассчитывается по следующей формуле 3:

$$a_{cmp} = \frac{O}{V}, \quad (3)$$

где «О – сумма обеспечения по страхованию, произведенного за три года, предшествующих текущему, (руб.);

V – сумма начисленных страховых взносов за три года, предшествующих текущему (руб.)» [21]:

$$V = \sum \Phi 3П t_{cmp}, \quad (4)$$

где $t_{стр}$ – «страховой тариф на обязательное социальное страхование от несчастных случаев на производстве и профессиональных заболеваний» [21].

$$V = \sum 6000000000 \cdot 0,007 = 42000000 \text{ руб}$$

$$a_{cmp} = \frac{300000}{42000000} = 0,007$$

Показатель $b_{стр}$ рассчитывается по формуле 5:

$$b_{cmp} = \frac{K \cdot 1000}{N}, \quad (5)$$

где K – «количество случаев, признанных страховыми за три года, предшествующих текущему;

N – среднесписочная численность работающих за три года, предшествующих текущему (чел.)» [21];

$$b_{cmp} = \frac{3 \cdot 1000}{3500} = 0,85$$

Показатель $c_{стр}$ рассчитывается по следующей формуле 6:

$$c_{cmp} = \frac{T}{S}, \quad (6)$$

где Т – «число дней временной нетрудоспособности в связи с несчастными случаями, признанными страховыми, за три года, предшествующих текущему;

S – количество несчастных случаев, признанных страховыми, исключая случаи со смертельным исходом, за три года, предшествующих текущему» [21].

$$c_{cmp} = \frac{125}{3} = 41,7$$

Коэффициент q_1 рассчитывается по следующей формуле 7:

$$q_1 = \frac{(q_{11} - q_{13})}{q_{12}}, \quad (7)$$

где q_{11} – «количество рабочих мест, в отношении которых проведена специальная оценка условий труда на 1 января текущего календарного года организацией, проводящей специальную оценку условий труда, в установленном законодательством Российской Федерации порядке;

q_{12} – общее количество рабочих мест;

q_{13} – количество рабочих мест, условия труда на которых отнесены к вредным или опасным условиям труда по результатам проведения специальной оценки условий труда» [21].

$$q_1 = \frac{3500 - 1200}{3500} = 0,66$$

Коэффициент q_2 рассчитывается по следующей формуле 8:

$$q_2 = \frac{q_{21}}{q_{22}}, \quad (8)$$

где q_{21} – «число работников, прошедших обязательные предварительные и периодические медицинские осмотры в соответствии с действующими нормативно-правовыми актами на 1 января текущего календарного года;

q_{22} – число всех работников, подлежащих данным видам осмотра, у страхователя» [21].

$$q_2 = \frac{3500}{3500} = 1$$

$$C(\%) = \left\{ 1 - \frac{\left(\frac{0,007}{0,12} + \frac{0,85}{0,94} + \frac{41,7}{85,73} \right)}{3} \right\} \cdot 0,66 \cdot 1 \cdot 100 = 34$$

Рассчитываем размер страхового тарифа на следующий год с учетом скидки или надбавки по формуле 9:

$$t_{стр}^{след} = t_{стр}^{тек} - t_{стр}^{тек} \cdot C, \quad (9)$$

$$t_{стр}^{след} = 0,7 - 0,7 \cdot 0,34 = 0,46$$

Рассчитываем размер страховых взносов по новому тарифу в следующем году по формуле 10:

$$V^{след} = \Phi \Pi^{тек} \cdot t_{стр}^{след}, \quad (10)$$

$$V^{2022} = 20000000000 \cdot 0,007 = 14000000 \text{ руб.}$$

$$V^{2022} = 20000000000 \cdot 0,0046 = 9200000 \text{ руб.}$$

Определяем размер экономии (роста) страховых взносов в следующем году по формуле 11:

$$\mathcal{E} = V^{тек} - V^{след} \quad (11)$$

$$\mathcal{E} = 14000000 - 9200000 = 4800000 \text{ руб.}$$

Оценка экономического эффекта определяется по формуле 12:

$$\mathcal{E}_e = \mathcal{E} - \mathcal{Z}_{ed} \quad (12)$$

где $\mathcal{Z}_{ed}$ – «единовременные затраты на проведение мероприятий по улучшению условия труда, руб» [21].

$$\mathcal{E}_e = 4800000 - 805000 = 3995000 \text{ руб.}$$

«Срок окупаемости затрат на проводимые мероприятия определяется соотношением суммы произведенных затрат к общему годовому экономическому эффекту» [21].

$$T_{ed} = \frac{\mathcal{Z}_{ed}}{\mathcal{E}_e} \quad (13)$$

$$T_{ed} = \frac{805000}{3995000} = 0,2 \text{ года}$$

Вывод по разделу.

В разделе определено, что экономический эффект от дополнения существующей системы контроля доступа в здания и помещения системами биометрической идентификации работников при помощи скана вен руки составит 3995000 руб. за счёт контроля нахождения работников в опасных зонах предприятия, а, соответственно, и снижения производственного травматизма.

Заключение

В первом разделе определено, чтобы гарантировать, что организационные и/или личные данные хорошо хранятся и доступны только назначенной стороне, необходимо реализовать защищенную биометрическую инфраструктуру. Крайне важно, чтобы был способ проверки только тех людей, которые определены как работники организации.

Особенностями биометрического контроля персонала заключается в том, что биометрические данные могут с вероятностью близкой к 100 % идентифицировать персонал в тех случаях, когда это необходимо для обеспечения безопасности.

Во втором разделе определено, что наибольшей популярностью среди биометрических технологий пользуется технология идентификации при помощи отпечатка пальца или руки, но при массовом сканировании необходимо прикасаться к поверхностям, которые могут быть загрязнены или заражены.

Определено, что для сканирования сетчатки глаза человеку необходимо снять очки, поднести глаз к сканеру, сфокусироваться на фиксированной точке и оставаться неподвижными в течение 10-15 секунд, что также в условиях массовой идентификации займёт большое количество времени.

Преимуществом технологии идентификации персонала по сосудистым рисункам руки является быстрота и отсутствие необходимости прикасаться к поверхностям сканеров.

Сканирование лица требует от работников снимать средства защиты (очки, маски, респираторы, каски, что в условиях химического производства может быть не безопасным.

Распознавание динамических подписей применима в основном для идентификации офисного персонала.

Технология распознавания голоса не применима в условиях повышенного шума на производстве.

В третьем разделе определено, что на опасный объект ООО «Тольяттикаучук» отсутствует автоматизированный СКУД для работников, которые не работают в помещениях данных объектов, а доступ работников осуществляется при помощи вызывной панели и радиобрелков. Из-за того, что часто работники забывают брелки доступ производится по вызывной панели.

Допуск в помещения с наличием токсичных жидких и газообразных продуктов только обученных работников правилам безопасности при нахождении в данных помещениях отделения позволит снизить количество несчастных случаев, производственного травматизма и заболеваний персонала ООО «Тольяттикаучук».

Для установки биометрического СКУД при входе в здание складского хозяйства и в помещения, где установлены линии подачи серной и азотной кислоты, а также реакторы Р-1, Р-2 и ёмкость маточного раствора в связи с тем, что работники постоянно носят СИЗ (перчатки, респираторы, очки, каски) предложена технология сканирования вен рук.

Выбор способа биометрической идентификации обусловлен:

- ношением касок, очков и других средств защиты лица (для сканирования черт лица не подходит);
- высокого уровня шума в помещениях предприятия (для сканирования голоса не подходит);
- гигиеническими требованиями (для сканирования отпечатка пальцев не подходит).

Разработана предлагаемая схема биометрической СКУД с использованием скана вен ладони руки.

В четвёртом разделе определено, что по результатам оценки рисков «высокий» риск выявлен на рабочем месте электромеханика в связи с опасностью воздействия электрического тока. Разработаны мероприятия по снижению всех идентифицированных рисков.

В пятом разделе определено, что загрязнение окружающей среды будет

минимальным при выдерживании заданных норм технологического режима на всех стадиях производства щавелевой кислоты, содержании в исправном состоянии технологического оборудования.

Основными целями деятельности объекта исследования в области обращения с отходами являются предотвращение вредного воздействия отходов производства и потребления, образующихся в процессе производственной деятельности на здоровье человека и окружающую природную среду.

В шестом разделе определено, что на ООО «Тольяттикаучук» специальным требованиям предусматриваются средства охраны.

При пожаре, аварийных ситуациях и стихийных бедствиях, пожарные и аварийные машины с расчетами, а также санитарные машины с медицинскими работниками допускаются на территорию объектов беспрепятственно с последующим информированием оперативно-производственной службы ООО «Тольяттикаучук». В остальных случаях доступ указанных транспортных средств осуществляется на общих основаниях. При выезде с территории объектов осмотр транспортных средств производится в установленном порядке.

На пожаро- и взрывоопасных объектах ООО «Тольяттикаучук» размещены технические средства, обеспечивающие взрывобезопасность процесса производства.

В седьмом разделе определено, что экономический эффект от дополнения существующей системы контроля доступа в здания и помещения системами биометрической идентификации работников при помощи скана вен руки составит 3995000 руб. за счёт контроля нахождения работников в опасных зонах предприятия, а, соответственно, и снижения производственного травматизма.

Список используемых источников

1. Девицына С. Н., Елецкая Т. А., Балабанова Т. Н., Гахова Н. Н. Разработка интеллектуальной системы биометрической идентификации пользователя // Экономика. Информатика. 2021. №1. С. 148-160.
2. Клычтаганов Ш. Биометрические системы // Символ науки. 2023. №10-2. С. 17-18. URL: <https://cyberleninka.ru/article/n/biometricheskie-sistemy> (дата обращения: 27.02.2025).
3. Мишунина Н. О. Разработка биометрической системы идентификации пользователя // APRIORI. Серия: Естественные и технические науки. 2023. №5. С. 12-39. URL: <https://cyberleninka.ru/article/n/razrabotka-biometricheskoy-sistemy-identifikatsii-polzovatelya> (дата обращения: 27.02.2025).
4. Назарова А. Д. Тенденции развития биометрических систем в России // Столыпинский вестник. 2023. №1. С. 22-37. URL: <https://cyberleninka.ru/article/n/tendentsii-razvitiya-tehnologiy-biometrii-v-rossii> (дата обращения: 27.02.2025).
5. Нечаева В. С. Идентификация отпечатков пальцев в биометрической системе безопасности // Вестник магистратуры. 2021. №5-3 (116). С. 65-66. URL: <https://cyberleninka.ru/article/n/indentifikatsiya-otpechatkov-paltsev-v-biometricheskoy-sisteme-bezopasnosti> (дата обращения: 27.02.2025).
6. О персональных данных [Электронный ресурс] : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024). URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=476043&ysclid=m7njooairk780093814> (дата обращения: 27.11.2024).
7. О противодействии терроризму [Электронный ресурс] : Федеральный закон от 06.03.2006 № 35-ФЗ. URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=486088> (дата обращения: 27.11.2024).
8. Об информации, информационных технологиях и о защите информации [Электронный ресурс] : Федеральный закон от 27.07.2006 № 149-

ФЗ.

URL:

<https://normativ.kontur.ru/document?moduleId=1&documentId=485876&ysclid=m7njolacrj46769607> (дата обращения: 27.11.2024).

9. Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты [Электронный ресурс] : Постановление Правительства РФ от 30.06.2018 № 772 (ред. от 12.07.2022). URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=471029&ysclid=m7njrpj0ujg168400295> (дата обращения: 27.11.2024).

10. Об отходах производства и потребления [Электронный ресурс]: Федеральный закон от 24.06.1998 №89-ФЗ (ред. от 04.08.2023). URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=444859&ysclid=h21gljcon369593919> (дата обращения: 27.11.2024).

11. Об охране атмосферного воздуха [Электронный ресурс] : Федеральный закон от 04.05.1999 № 96-ФЗ (ред. от 13.06.2023). URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=400412&ysclid=h21ft3yhi17986064> (дата обращения: 27.11.2024).

12. Об утверждении Правил поведения, обязательных для исполнения гражданами и организациями, при введении режима повышенной готовности или чрезвычайной ситуации [Электронный ресурс]: Постановление Правительства РФ от 02.04.2020 № 417. URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=358723&ysclid=m7hqxiaqjo741186284> (дата обращения: 08.09.2024).

13. Об утверждении Примерного положения о системе управления охраной труда [Электронный ресурс] : Приказ Минтруда России от 29.10.2021 № 776н. URL:

<https://normativ.kontur.ru/document?moduleId=1&documentId=409457&ysclid=ld8jp94kat939272210> (дата обращения: 27.11.2024)

14. Об утверждении рекомендаций по выбору методов оценки уровней профессиональных рисков и по снижению уровней таких рисков [Электронный ресурс] : Приказ Минтруда России от 28.12.2021 № 926. URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=411523&ysclid=ld8jqdwcm8100411018> (дата обращения: 05.11.2024).

15. Об утверждении Федерального классификационного каталога отходов [Электронный ресурс] : Приказ Федеральной службы по надзору в сфере природопользования от 22.05.2017 № 242. URL: <http://docs.cntd.ru/document/542600531> (дата обращения: 27.11.2024).

16. Об утверждении формы отчета об организации и о результатах осуществления производственного экологического контроля [Электронный ресурс] : Приказ Минприроды России от 15.03.2024 № 173. URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=472325> (дата обращения: 05.11.2024).

17. Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования [Электронный ресурс]: СП 132.13330.2011. URL: <https://www.minstroyrf.gov.ru/docs/1959/> (дата обращения: 27.08.2024).

18. Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки [Электронный ресурс]. URL: <https://www.garant.ru/products/ipo/prime/doc/70342932/?ysclid=mben78mfil756466439> (дата обращения: 12.11.2024).

19. Система стандартов безопасности труда. Пожарная безопасность. Общие требования [Электронный ресурс] : ГОСТ 12.1.004-91. URL: <https://internet-law.ru/gosts/gost/3254/?ysclid=lga9r9fn5z366382597> (дата обращения: 12.11.2024).

20. Трудовой кодекс Российской Федерации [Электронный ресурс] : Федеральный закон от 30.12.2001 № 197-ФЗ. URL: <http://docs.cntd.ru/document/901807664> (дата обращения: 27.11.2024).

21. Фрезе Т. Ю. Оценка эффективности мероприятий по обеспечению техносферной безопасности. Выполнение раздела выпускной квалификационной работы по направлению подготовки 20.03.01 «Техносферная безопасность» : электронное учебно-методическое пособие / Т.Ю. Фрезе. Тольятти : Изд-во ТГУ, 2022. 1 оптический диск. ISBN 978-5-8259-1456-5.

Приложение А

Паспорт безопасности

ПАСПОРТ БЕЗОПАСНОСТИ

ООО «Тольяттикаучук»

(наименование объекта (территории))

г. Тольятти

(наименование населенного пункта)

2025 г.

I. Общие сведения об объекте (территории)

ПАО «Татнефть»

(наименование органа (организации), в ведении которого находится объект (территория), адрес, телефон, факс, адрес электронной почты)

445007, Самарская область, город Тольятти, Новозаводская ул., д.8

(адрес объекта (территории), телефон, факс, адрес, электронной почты)

Производство синтетического каучука

(основной вид деятельности органа (организации), в ведении которого находится объект (территория))

Первая категория

(категория объекта (территории))

2000000 м²

(общая площадь объекта (территории), кв. метров, протяженность периметра, метров)

-

(сведения о государственной регистрации права на объект недвижимого имущества)

Морозов Юрий Витальевич

(ф.и.о. должностного лица, осуществляющего непосредственное руководство деятельностью работников на объекте (территории), служебный и (или) мобильный телефоны, факс, адрес электронной почты)

-

(ф.и.о. руководителя органа (организации), в ведении которого находится объект (территория), служебный и (или) мобильный телефоны, факс, адрес электронной почты)

II. Сведения о работниках (сотрудниках) объекта (территории) и иных лицах, находящихся на объекте (территории)

1. Режим работы объекта (территории)

ежедневно с 08:00 до 22:00

(продолжительность, начало и окончание рабочего дня)

2. Общее количество работников (сотрудников) объекта (территории) 3693. (человек)

Продолжение Приложения А

3. Среднее количество находящихся на объекте (территории) в течение рабочего дня работников (сотрудников) объекта (территории), работников (сотрудников), осуществляющих охрану объекта (территории), арендаторов и иных лиц, осуществляющих безвозмездное пользование имуществом, находящимся на объекте (территории), 2500. (человек)

4. Среднее количество находящихся на объекте (территории) в нерабочее время, ночью, в выходные и праздничные дни работников (сотрудников) объекта (территории), работников (сотрудников), осуществляющих охрану объекта (территории), арендаторов и иных лиц, осуществляющих безвозмездное пользование имуществом, находящимся на объекте (территории), 180. (человек)

5. Сведения об арендаторах и иных лицах, осуществляющих безвозмездное пользование имуществом, находящимся на объекте (территории)

Арендаторы отсутствуют

(полное и сокращенное наименование организации, основной вид деятельности, общее количество работников (сотрудников), расположение рабочих мест на объекте (территории), занимаемая площадь (кв. метров), режим работы, ф.и.о., номера телефонов (служебного, мобильного) руководителя организации, срок действия аренды и (или) иные условия нахождения (размещения) на объекте (территории))

III. Сведения о потенциально опасных участках и (или) критических элементах объекта (территории)

1. Потенциально опасные участки объекта (территории) (при наличии)

Наименование	Количество человек, находящихся на участке, человек	Общая площадь, кв. метров	Характер террористической угрозы	Характер возможных последствий
Здание заводоуправления	250 человек	5500	Захват заложников	Взрыв, гибель, ранения заложников

2. Критические элементы объекта (территории) (при наличии)

Наименование	Количество человек, находящихся на участке, человек	Общая площадь, кв. метров	Характер террористической угрозы	Характер возможных последствий
Товарно-сырьевой цех	25	5800	Взрыв	Разрушение ёмкостей и зданий насосных

Продолжение Приложения А

3. Возможные места и способы проникновения на объект (территорию)

Периметр территории, КПП

4. Наиболее вероятные средства поражения, которые могут применяться при совершении террористического акта

Взрывные устройства, ЛВЖ и ГЖ

IV. Прогноз последствий совершения террористического акта на объекте (территории)

1. Предполагаемые модели действий нарушителей

Взятие заложников, поджог

(краткое описание основных угроз совершения террористического акта на объекте (территории), возможность размещения на объекте (территории) взрывных устройств, захват заложников из числа работников и иных лиц, находящихся на объекте (территории), наличие рисков химического, биологического и радиационного заражения (загрязнения))

2. Возможные последствия совершения террористического акта на объекте (территории)

Площадь возможной зоны разрушения (заражения) в случае совершения террористического акта составит 5800 м²

(площадь возможной зоны разрушения (заражения) в случае совершения террористического акта, кв. метров, иные ситуации в результате совершения террористического акта)

3. Оценка социально-экономических последствий совершения террористического акта на объекте (территории)

Возможные людские потери, человек	Возможные нарушения инфраструктуры	Возможный экономический ущерб, рублей
До 250 человек	Разрушение зданий, разрушение систем жизнеобеспечения	До 150 млн. рублей

V. Силы и средства, привлекаемые для обеспечения антитеррористической защищенности объекта (территории)

1. Силы, привлекаемые для обеспечения антитеррористической защищенности объекта (территории)

Физическая охрана объекта осуществляется сотрудниками ЧОП в количестве 25 чел.

Продолжение Приложения А

2. Средства, привлекаемые для обеспечения антитеррористической защищенности объекта (территории)

Специальные средства и вооружение (гражданское и служебное оружие)

VI. Меры по инженерно-технической, физической защите и пожарной безопасности объекта (территории)

1. Меры по инженерно-технической защите объекта (территории):

а) объектовые и локальные системы оповещения

Носимые радиостанции Motorola

(наличие, марка, характеристика)

б) резервные источники электро-, тепло-, газо- и водоснабжения, систем связи

Цех электроснабжения с двумя независимыми подключениями энергоснабжения

(наличие, количество, характеристика)

в) технические системы обнаружения несанкционированного проникновения на объект (территорию), оповещения о несанкционированном проникновении на объект (территорию) или системы физической защиты

Система охранной сигнализации

(наличие, марка, количество)

г) стационарные и ручные металлоискатели

Стационарные ручные металлоискатели – 9 шт.

Ручные металлоискатели – 13 шт.

(наличие, марка, количество)

д) телевизионные системы охраны

Система телевизионного видеонаблюдения на базе оборудования Bolid

(наличие, марка, количество)

е) системы охранного освещения

Видеонаблюдение при помощи 44 видеокамер.

(наличие, марка, количество)

2. Меры по физической защите объекта (территории):

а) количество контрольно-пропускных пунктов (для прохода людей и проезда транспортных средств)

Количество постов – 2; проходные – 2

Продолжение Приложения А

б) количество эвакуационных выходов (для выхода людей и выезда транспортных средств)

2 эвакуационных выхода

в) электронная система пропуска

СКУД

(наличие, тип установленного оборудования)

г) укомплектованность личным составом нештатных аварийно-спасательных формирований (по видам подразделений)

Нет

(человек, процентов)

3. Меры по обеспечению пожарной безопасности объекта (территории):

а) наружное противопожарное водоснабжение

Система противопожарного наружного водоснабжения (кольцевая) диаметром 250 мм

(наличие, тип, характеристика)

б) внутреннее противопожарное водоснабжение

Внутренний пожарный водопровод, совмещенный с хозяйственно-питьевым водопроводом.

(наличие, тип, характеристика)

в) автоматическая установка пожарной сигнализации

Адресная АПС «Сигнал-20» – обнаружение пожара

(наличие, тип, характеристика)

г) автоматическая установка пожаротушения

Отсутствует

(наличие, тип, характеристика)

д) система противодымной защиты

Отсутствует

(наличие, тип, характеристика)

е) система оповещения и управления эвакуацией людей при пожаре

СОУЭ второго типа

(наличие, тип, характеристика)

Продолжение Приложения А

ж) противопожарное состояние путей эвакуации и эвакуационных выходов

Эвакуационные пути и выходы соответствуют требованиям

(количество, параметры)

4. План взаимодействия с территориальными органами безопасности, территориальными органами МВД России и территориальными органами Росгвардии по защите объекта (территории) от террористических угроз

Отсутствует

(наличие, реквизиты документа)

VII. Выводы и рекомендации

-

VIII. Дополнительная информация с учетом особенностей объекта (территории)

-

(наличие на объекте (территории) режимно-секретного органа, его численность (штатная и фактическая), количество сотрудников объекта (территории), допущенных к работе со сведениями, составляющими государственную тайну, меры по обеспечению режима секретности и сохранности секретных сведений)

-

(наличие на объекте (территории) локальных зон безопасности)

-

(другие сведения)