МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНЖЕНЕРНАЯ ШКОЛА
КАФЕДРА ТРАНСПОРТНЫХ ПРОЦЕССОВ И ТЕХНОЛОГИЙ

ОТЧЕТ ПО УЧЕБНОЙ ПРАКТИКЕ ПО ПОЛУЧЕНИЮ НАВЫКОВ ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ

Студент
гр. БТТ-24-ЭУ1 _____ М.А. Соколов

Руководитель
ассистент _____ К.Б. Карсаков

Хорошо

Владивосток 2025

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНЖЕНЕРНАЯ ШКОЛА
КАФЕДРА ТРАНСПОРТНЫХ ПРОЦЕССОВ И ТЕХНОЛОГИЙ

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

на учебную практику по получению навыков исследовательской работы

Студент(-ка) группы БТТ-24-ЭУ1 Соколов Михаил Алексеевич.

Направление подготовки: 23.03.01 Технология транспортных процессов

Профиль: Экономика и управление на транспорте

Место прохождения практики: ФГБОУ ВО «ВВГУ», Инженерная школа, кафедра транспортных процессов и технологий, г. Владивосток, ул. Гоголя, 41.

Период прохождения практике: с «10» февраля 2025 г. по «28» июня 2025 г.

Целью практики является закрепление полученных знаний и профессиональных навыков в профильном виде деятельности, сбор материала для подготовки и написания отчета по практике.

Задание:

№	Содержание
1	Знакомство с методами научного исследования
2	Изучить нормативно-правовую базу по теме, заданной руководителем
3	Выявить проблемные области по теме практики
4	Провести работу с научной, профессионально-технической и учебно-методической литературой, в том числе осуществить поиск необходимой информации в сети Интернет
5	Предложить варианты решения проблем(-ы)
6	Систематизировать и обобщить материалы для включения в отчет
7	Написать отчет по учебной практике по получению навыков исследовательской работе
8	Защитить работу

Руководитель ОО
Ассистент кафедры ТПТ _____ Карсаков К.Б.
(Фамилия И.О.)

Задание получил _____
(Соколов М.А.)

Дата выдачи задания 10.02.2025

Содержание

Введение.....3
1 Основная часть.....5
1.1 История развития автономных складов.....5
1.2 Основной функционал автономного склада.....6
2 Современное состояние автономных складов.....10
2.1 Текущее состояние безопасности автономных складов.....10
2.2 Основные киберугрозы в условиях автоматизированных складских комплексов10
2.3 Меры по предотвращению кибератак.....11
2.4 Основные физические угрозы в условиях автономных складов.....12
2.5 Основные техногенные риски автоматизированных складов.....13
2.6 Меры по предотвращению техногенных катастроф.....14
Заключение.....17
Список использованных источников.....19

Введение

Автоматизированные склады представляют собой высокотехнологичные логистические комплексы, где процессы приёмки, хранения, комплектации и отгрузки товаров осуществляются с помощью автоматических систем и роботизированных технологий при минимальном участии человека.

Актуальность вопросов их безопасности стремительно возрастает в условиях цифровизации логистики и роста угроз различного характера. Сегодня такие объекты становятся критически важными звеньями глобальных цепей поставок, а их уязвимость может привести к серьезным экономическим потерям и нарушениям в работе целых отраслей.

Основная проблема заключается в том, что традиционные подходы к защите складских помещений уже не соответствуют современным вызовам. Автоматизированные системы управления, роботизированные погрузчики и системы компьютерного зрения, обеспечивающие бесперебойную работу склада, одновременно создают новые векторы для потенциальных атак. Благодаря им киберпреступники, способны дистанционно нарушать работу оборудования, похищать конфиденциальные данные или полностью парализовать работу логистических центров.

Современные автономные складские комплексы сталкиваются с серьезными вызовами в области физической безопасности. Ограниченное присутствие персонала создает благоприятные условия для злоумышленников, при этом традиционные системы видеонаблюдения и контроля доступа часто работают изолированно от киберзащиты, образуя опасные «слепые зоны».

Особую озабоченность вызывают комбинированные угрозы, когда физическое проникновение сопровождается кибератакой на систему управления. Эта уязвимость усугубляется тем, что современные автоматизированные склады представляют собой сложные технологические комплексы, где даже незначительный инцидент может вызвать каскадный сбой логистических процессов.

Техногенные риски, включая пожары, перебои электроснабжения и отказы оборудования, требуют принципиально новых подходов к обеспечению безопасности. Существующие системы аварийного реагирования зачастую не адаптированы к специфике полностью автономных объектов, где традиционные методы эвакуации и локализации чрезвычайных ситуаций оказываются неэффективными.

Одним из самых сложных является человеческий фактор – от ошибок программирования и неправильной настройки оборудования до умышленных действий

недобросовестных сотрудников. При этом существующие нормативные документы и отраслевые стандарты зачастую не поспевают за стремительным развитием складских технологий, оставляя многие аспекты безопасности на усмотрение операторов.

Целью работы является разработка интегрированной системы безопасности для автоматизированных складов, объединяющей физическую защиту, кибернетическую устойчивость и интеллектуальный мониторинг угроз в единый автоматизированный комплекс.

Исследование направлено на создание «умной» системы на основе технологий искусственного интеллекта и машинного обучения, способной в режиме реального времени анализировать данные, прогнозировать потенциальные угрозы и автоматически реагировать на нештатные ситуации – от несанкционированного доступа до кибератак на систему управления складом.

Особое внимание уделяется разработке превентивных механизмов защиты, минимизирующих необходимость человеческого вмешательства.

Результатом исследования станет методология построения комплексной системы безопасности, обеспечивающей не только защиту материальных активов, но и бесперебойность критически важных логистических процессов на автоматизированных складах. Практическая значимость работы заключается в возможности внедрения разработанных решений в существующую складскую инфраструктуру с целью повышения её отказоустойчивости и безопасности.

1 Основная часть

1.1 История развития автономных складов

Первый этап развития автономных складов относится к послевоенному периоду 1950-1970-х годов, когда началось внедрение первых механизированных систем на складских объектах. В этот период произошла революция в организации складского хозяйства – на смену ручному труду пришли конвейерные ленты для перемещения грузов, электрические тележки и первые системы палетного хранения. Особое значение имело изобретение в 1962 году немецкой компанией Demag первых автоматизированных кранов-штабелеров, которые стали прообразом систем автоматизированного складирования (САС). Эти технологические новшества позволили значительно увеличить плотность хранения грузов и сократить время выполнения складских операций, хотя уровень автоматизации оставался относительно низким, а большинство процессов по-прежнему требовали участия человека. Пример организации автоматизированного производства указан на рисунке 1.

Рисунок 1 – Конвейерная автоматизация производства

Следующий важный этап эволюции пришелся на 1980-1990-е годы и был связан с активной компьютеризацией складских комплексов. В этот период появились первые полноценные системы управления складом (СУС), которые радикально изменили подходы к учету и контролю товарных запасов. Широкое внедрение штрихкодирования и систем радио-идентифицирования позволило автоматизировать процессы идентификации и инвентаризации товаров. Знаковым событием стало появление автоматизированных стеллажных систем (АСС) с программным управлением, где краны-штабелеры могли самостоятельно перемещать грузы по заданным алгоритмам. К концу 1990-х годов крупные ритейлеры, включая Amazon, начали создавать первые полуавтоматические склады, где часть операций (в первую очередь сортировка) выполнялась машинами, хотя ключевые процессы по-прежнему требовали человеческого участия.

Настоящий прорыв в развитии автономных складов произошел в 2000-2010-х годах благодаря революции в области робототехники и искусственного интеллекта. Появление автономных мобильных роботов, таких как разработки компании «Kiva Systems» (приобретенной Amazon в 2012 году), позволило автоматизировать процессы комплектации и перемещения грузов. В этот период началось активное использование дронов для инвентаризации складов, а алгоритмы машинного обучения стали применяться для оптимизации маршрутов перемещения и прогнозирования спроса. Технологический прогресс привел к созданию первых практически полностью автоматизированных складских комплексов, где до 80% операций выполнялось без человеческого вмешательства.

Современный этап развития (2020-е годы) характеризуется стремлением к созданию полностью автономных складских систем. Ведущие логистические компании, такие как Wildberries и OZON, уже эксплуатируют склады, где 70% процессов – от приемки товаров до их отгрузки – выполняются роботизированными системами. Пример автоматизированного склада указан на рисунке 2.

Рисунок 2 – Автоматизированный склад Wildberries

Современные технологии искусственного интеллекта (ИИ) становятся ключевым инструментом в управлении складскими комплексами, обеспечивая не только автоматизацию рутинных операций, но и интеллектуальный анализ данных для стратегического планирования. С помощью машинного обучения и нейросетевых алгоритмов системы ИИ способны с высокой точностью прогнозировать спрос, учитывая сезонные колебания, рыночные тренды и даже внешние факторы, такие как экономическая ситуация или изменения в поведении потребителей. Это позволяет компаниям оптимизировать товарные запасы, минимизировать издержки и предотвращать как избыточное складирование, так и дефицит продукции.

Одним из наиболее инновационных направлений в этой сфере стало внедрение цифровых двойников (Digital Twins) — виртуальных копий складских комплексов, которые в реальном времени отражают все физические процессы, происходящие на объекте.

Эти модели позволяют тестировать различные сценарии работы, начиная от перепланировки складских зон до имитации пиковых нагрузок, без риска для реальных операций. Например, с помощью цифрового двойника можно заранее оценить, как изменение логистических маршрутов повлияет на скорость обработки заказов, или как внедрение новых роботизированных систем скажется на общей производительности.

Перспективы развития автономных складов выходят далеко за рамки простой автоматизации. В ближайшем будущем ожидается полный отказ от человеческого присутствия в складских помещениях — все процессы, от приемки товара до отгрузки, будут выполнять роботизированные системы, управляемые ИИ.

Биометрические системы безопасности, такие как распознавание лиц, голоса или даже походки, обеспечат надежный контроль доступа и предотвратят несанкционированное проникновение.

Кроме того, развитие квантовых вычислений открывает новые горизонты для управления логистикой: квантовые алгоритмы смогут мгновенно анализировать огромные массивы данных, оптимизировать маршруты доставки и прогнозировать возможные сбои в цепях поставок с беспрецедентной точностью.

1.2 Основной функционал автономного склада

Автономные склады нового поколения представляют собой высокотехнологичные логистические комплексы, где все ключевые процессы – от приемки товара до его отгрузки – осуществляются с минимальным участием человека. Основу таких складов составляют автоматизированные системы управления складом (СУС), которые в реальном времени координируют работу роботизированных погрузчиков, конвейерных линий и систем хранения.

Современные склады оснащаются интеллектуальными системами, которые благодаря компьютерному зрению и алгоритмам машинного обучения автоматически распознают товары по штрихкодам, радиометкам или даже визуальным характеристикам, минимизируя ошибки, связанные с ручным вводом данных. Эти технологии не только ускоряют процессы приемки, сортировки и инвентаризации, но и обеспечивают высокую точность учета, адаптируясь к различным типам упаковки и условиям хранения. Датчики интернет вещей, интегрированные в складскую инфраструктуру, собирают данные в режиме реального времени, анализируя не только базовые параметры, такие как температура и влажность, но и более сложные показатели – уровень вибрации, освещенности или содержание газов в воздухе, что особенно важно для чувствительных товаров, например, фармацевтической продукции или электронных компонентов.

Центральным элементом автономного склада является система автоматизированного складирования (САС), включающая высотные стеллажные системы с автоматическими штабелерами. Пример САС указан на рисунке 3.

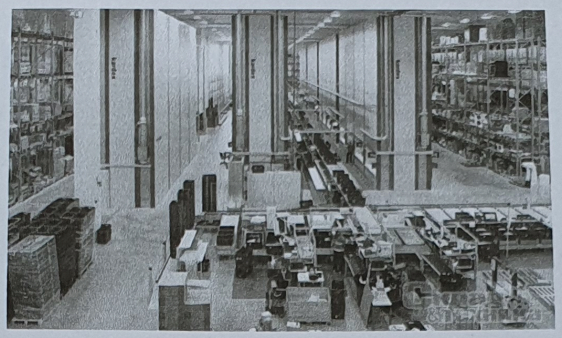

Рисунок 3 – Система автоматизированного складирования (САС)

Современные автономные складские комплексы представляют собой вершину технологической эволюции логистики, где каждый процесс оптимизирован до совершенства. Основу их работы составляют высокоточные автоматизированные системы, способные с высокой точностью (до миллиметра) перемещать грузовые паллеты массой в несколько тонн, работая в полностью автономном режиме без постоянного контроля оператора. Для обеспечения такой точности используются многоуровневые системы навигации, сочетающие старые технологии (магнитные направляющие, оптические сенсоры) с передовыми решениями (лидарные системы, ультразвуковые датчики пространственного позиционирования и 3D-камеры компьютерного зрения). Особое внимание в современных проектах уделяется энергоэффективности – инновационные системы рекуперации энергии позволяют возвращать до 30% затраченной мощности при торможении грузоподъемных механизмов, что в сочетании с «умными» системами энергоменеджмента дает до 40% экономии на эксплуатационных расходах по сравнению с традиционными складами.

Логистическая философия автономных складов реализует принципиально новый подход «от товара к человеку», радикально меняющий традиционные представления о складской работе. Вместо того чтобы операторы перемещались между стеллажами, сложные алгоритмы динамической маршрутизации обеспечивают доставку нужных товаров к стационарным рабочим станциям. Эти интеллектуальные системы учитывают сотни параметров в реальном времени: от приоритетности заказов и сроков отгрузки до оптимальных траекторий движения техники, позволяющих минимизировать энергозатраты и время обработки. Прогнозные аналитические системы на базе машинного обучения анализируют исторические данные, сезонные тренды и даже погодные условия, заранее оптимизируя схему размещения товаров. Наиболее прогрессивные «темные склады» доводят

концепцию автоматизации до абсолютного уровня – все операции выполняются в полностью автономном режиме без необходимости постоянного освещения рабочих зон, что дает дополнительную экономию энергии и создает идеальные условия для хранения светочувствительной продукции.

Надежность работы таких комплексов обеспечивается многослойной системой защиты и резервирования. Все критические компоненты имеют как минимум дублирующие аналоги, а системы энергоснабжения включают несколько независимых контуров: от традиционных дизель-генераторов и промышленных аккумуляторных батарей до солнечных панелей и других возобновляемых источников энергии. Централизованная система мониторинга в режиме реального времени анализирует тысячи параметров работы оборудования, используя технологии предиктивной аналитики для заблаговременного выявления потенциальных неисправностей. Кибербезопасность обеспечивается комплексом мер: физически изолированными промышленными сетями, системами многофакторной биометрической аутентификации, постоянным криптографическим аудитом и «песочницами» для тестирования всех программных обновлений.

Эффективность автономных складов устанавливает новые отраслевые стандарты. Точность выполнения заказов достигает беспрецедентных 99,99%, что практически исключает ошибки комплектации. Скорость обработки заказов в 2-3 раза выше, чем на традиционных складах, при этом производительность остается стабильной 24 часа в сутки, 365 дней в году, без перерывов на обед, выходные или праздники. Гибкость системы позволяет мгновенно адаптироваться к изменениям – будь то резкий рост нагрузки в предпраздничный период или необходимость перестройки логистических процессов под новые категории товаров.

Современные автономные склады способны самостоятельно проводить полную инвентаризацию за считанные часы (вместо нескольких дней на традиционных складах), генерировать аналитические отчеты в реальном времени и прогнозировать необходимость технического обслуживания оборудования, минимизируя простои.

2 Современное состояние автономных складов

2.1 Текущее состояние безопасности автономных складов

Современные автономные складские комплексы, несмотря на впечатляющий уровень технологической оснащенности и автоматизации процессов, сталкиваются с целым комплексом взаимосвязанных угроз безопасности, требующих комплексного системного подхода к их предотвращению и минимизации последствий. В условиях стремительной цифровизации логистических процессов особую актуальность приобретают кибернетические угрозы, связанные с потенциальными атаками на программное обеспечение систем управления складом (СУС), промышленные контроллеры и сети передачи данных. Физические угрозы проникновения усугубляются особенностями архитектуры автономных складов – минимальным количеством персонала на территории и высокой степенью зависимости от автоматизированных систем контроля доступа. Отдельную категорию рисков составляют техногенные опасности, включающие в себя как традиционные угрозы вроде пожаров и перебоев электроснабжения, так и специфические риски, характерные именно для автоматизированных комплексов, такие как массовые сбои в работе роботизированного оборудования или отказы систем позиционирования автономных транспортных средств.

Киберугрозы для автономных складов представляют особую опасность в силу высокой степени интеграции цифровых систем и физических процессов. Успешная хакерская атака может привести не просто к утечке данных, но и к реальным физическим повреждениям оборудования, нарушениям логистических процессов и значительным финансовым потерям. Физические угрозы в условиях автономных складов приобретают новые формы – от классических попыток несанкционированного проникновения до изощренных методов обхода биометрических систем контроля доступа.

Техногенные риски в свою очередь требуют принципиально новых подходов к обеспечению безопасности, так как традиционные системы противопожарной защиты и аварийного реагирования зачастую не учитывают специфику полностью автоматизированных объектов. Особую сложность представляет комбинированный характер современных угроз, когда кибератака может спровоцировать техногенную аварию, а физическое проникновение – создать условия для кибернетического взлома.

2.2 Основные киберугрозы в условиях автоматизированных складских комплексов

В эпоху цифровой трансформации логистики киберугрозы становятся наиболее критичным вызовом для полностью автоматизированных складских комплексов. Полная

зависимость современных складов от программных систем управления создает беспрецедентные риски – успешная хакерская атака способна полностью парализовать работу всего предприятия. Особую опасность представляют целевые атаки на промышленные контроллеры, которые могут привести к физическому повреждению оборудования. 10 марта в 2022 году зафиксирован случай, по информации Ассоциации организаций продуктового сектора (АСОРПС) хакеры совершили атаку на оборудование, управляющее хладогенераторными установками агрохаба «Селятино» в Московской области. Они пытались испортить 40 тысяч тонн замороженной продукции.

Атака совершена, предположительно, группировкой «Anonymous» рано утром 26 февраля. Об этом сообщила компания «Славтранс-Сервис», член АСОРПС.

«Был получен несанкционированный доступ к головному контроллеру под пользователем «Supervisor». В 00:27 был создан пользователь «Anonymous» с полными правами. После чего были изменены ключевые параметры, отвечающие за поддержание температуры с -24° С на +30° С с целью порчи 40 тысяч тонн замороженной мясной и рыбной продукции. Оборудование имело доступ в сеть интернет для удаленного мониторинга за работой установок» – говорится в письме, направленном «Славтранс-Сервис» в Минсельхоз РФ.

Служба безопасности агрохаба оперативно отразила атаку, восстановив исходные параметры и сохранив продукцию в полном объеме. Сейчас холодильно-складской комплекс отключен от интернета и переведен на локальное управление. АО «Славтранс-Сервис» входит в Ассоциацию организаций продуктового сектора (АСОРПС). Высокотехнологичный комплекс в Селятино под Наро-Фоминском площадью более 8000 м² рассматривается как один из опорных элементов транспортного коридора между Россией и КНР.

Также не менее распространены атаки типа «посредник», когда перехватывается связь между операторами и автоматизированной техникой.

Реальную проблему представляет и вредоносное ПО, специально разработанное для срыва логистических операций – такие программы могут фальсифицировать данные инвентаризации, блокировать системы сортировки или искажать маршруты автоматических погрузчиков. Отсутствие оперативного персонала на территории усугубляет последствия таких инцидентов, так как время реагирования критически увеличивается.

2.3 Меры по предотвращению кибератак

Для защиты от кибератак необходимо внедрение многоуровневой системы аутентификации, сегментация сетей управления и постоянный мониторинг сетевой активности с использованием технологий машинного обучения для выявления

подозрительных действий. Особое внимание следует уделить резервированию критически важных систем – дублирование источников питания, создание отказоустойчивых архитектур управления и наличие планов аварийного перехода на ручное управление в экстренных ситуациях.

Перспективным направлением повышения безопасности является разработка и внедрение систем предиктивной аналитики, способных на основе анализа больших данных предсказывать возможные сбои и аварийные ситуации. Такие системы, интегрированные с цифровыми двойниками складских комплексов, позволят моделировать потенциально опасные сценарии и разрабатывать превентивные меры защиты. Важным аспектом является стандартизация подходов к безопасности автономных складов – разработка единых отраслевых стандартов и протоколов, которые обеспечат совместимость систем безопасности различных производителей и позволят создать единое защищенное пространство для логистических комплексов будущего.

Реализация этих мер требует тесного взаимодействия разработчиков автоматизированных систем, специалистов по кибербезопасности и эксплуатационного персонала, что подчеркивает необходимость междисциплинарного подхода к обеспечению безопасности автономных складских комплексов.

2.4 Основные физические угрозы в условиях автономных складов

Парадокс современных автоматизированных складов заключается в том, что снижение человеческого присутствия, с одной стороны повышает безопасность (меньше возможностей для внутренних хищений), с другой – создает новые уязвимости для внешних нарушителей. Злоумышленники могут использовать различные методы обхода систем контроля доступа – от подделки биометрических данных до физического повреждения сенсоров. Зафиксированы случаи, когда преступники специально провоцировали ложные срабатывания противопожарных систем, чтобы создать хаос и проникнуть на охраняемую территорию.

Отдельную проблему представляет физическое вмешательство в работу роботизированного оборудования, которое может повлечь за собой нарушение работы автономных систем. Особую опасность представляет возможность комбинированных атак, когда физическое проникновение сочетается с кибервоздействием – например, подключение к внутренним сетям через незащищенные интерфейсы обслуживания оборудования с последующим проникновением на склад.

Традиционные системы видеонаблюдения часто оказываются неэффективными в условиях больших площадей и сложной конфигурации современных складских комплексов.

Неэффективность систем наблюдения может представлять собой наличие слепых зон, ошибки в программном обеспечении оборудования или его технической неисправности.

2.5 Основные техногенные риски автоматизированных складов

Высокая технологичность современных складских комплексов порождает техногенные риски, требующие особых подходов к безопасности. Проблема возгораний литий-ионных аккумуляторов в автономных роботах является настоящей проблемой в отрасли автономных складских помещений, поскольку эти действия могут повлечь за собой неконтролируемый пожар на складском помещении. Также существует высокий риск пожара в связи неисправностью электрооборудования, который может повлечь за собой катастрофические последствия, если инцидент не получится локализовать.

Так, например в ночь на Субботу, 13 января, недалеко от Санкт-Петербурга – в Шушарах – начинается пожар на складе одного из крупнейших маркетплейсов страны. Пламя охватывает весь комплекс площадью 70 тысяч квадратных метров. Дым накрыл южную часть города и был виден на расстоянии десятков километров. Возгоранию присвоили самый высокий – пятый ранг сложности. На то, чтобы окончательно справиться с огнем, понадобились почти сутки. Последствия пожара на складе Wilberries можно посмотреть на рисунке 4.

Рисунок 4 – Пожар на складе «Wildberries»

Современные автоматизированные системы обладают высокой степенью энергозависимости, что формирует серьезную уязвимость в их работе – даже кратковременные перебои в электроснабжении продолжительностью всего 10-15 минут способны спровоцировать цепную реакцию сбоев, затрагивающую все технологические процессы предприятия. В условиях высокой автоматизации механические поломки становятся особенно критичными, учитывая сокращенный штат обслуживающего персонала – например, заклинивший кран-штабелер способен полностью парализовать работу целого складского сектора на несколько часов, вызывая значительные логистические задержки и

финансовые потери.

Климатическое оборудование также представляет собой существенный источник рисков – отказ холодильных установок на фармацевтическом или продовольственном складе может привести к необратимой порче термочувствительной продукции на суммы, исчисляемые миллионами рублей. Особую сложность представляет каскадный характер современных техногенных угроз, когда даже незначительная, на первый взгляд, неисправность способна инициировать цепочку взаимосвязанных событий, в конечном итоге приводящую к полному нарушению функционирования всего производственного или логистического комплекса.

При этом традиционные системы безопасности зачастую не рассчитаны на столь сложные сценарии развития аварийных ситуаций, поскольку они, как правило, реагируют на уже произошедшие инциденты, а не предотвращают их на ранних стадиях.

Для эффективного противодействия этим угрозам требуется внедрение многоуровневой системы безопасности, интегрирующей в себе различные защитные механизмы. Ключевым элементом такой системы должна стать платформа киберфизической безопасности, обеспечивающая комплексный мониторинг как физической, так и цифровой инфраструктуры. В рамках этой платформы данные с видеокамер, датчиков движения, температурных и вибрационных сенсоров должны анализироваться в реальном времени вместе с показателями состояния информационных систем, сетевой активности и работоспособности промышленного оборудования.

2.6 Меры по предотвращению техногенных катастроф

Современные автоматизированные складские комплексы, представляя собой сложные технологические системы, требуют особого внимания к вопросам техногенной безопасности. Высокая степень автоматизации, интенсивное использование роботизированной техники и плотное размещение товарных запасов создают уникальные вызовы в области предотвращения катастрофических ситуаций. Однако современный уровень развития технологий безопасности позволяет эффективно нейтрализовать эти риски при условии реализации комплексного подхода, охватывающего все аспекты функционирования складского комплекса.

Основой системы предотвращения техногенных катастроф выступает интеллектуальная система мониторинга, представляющая собой распределенную сеть из сотен датчиков, непрерывно отслеживающих все критически важные параметры работы склада. Эти сенсоры, оснащенные технологиями интернет вещей, контролируют не только традиционные показатели (температуру, влажность, загазованность), но и такие

специфические параметры, как вибрационное состояние оборудования, степень износа ключевых узлов, уровень заряда аккумуляторных батарей и даже микроскопические утечки охлаждающих жидкостей. Особое внимание уделяется зонам повышенного риска – местам зарядки аккумуляторов, электрощитовым помещениям и участкам хранения опасных грузов, где устанавливаются датчики с повышенной чувствительностью и частотой опроса. Современные алгоритмы машинного обучения анализируют поступающие данные в реальном времени, выявляя малейшие отклонения от нормальных показателей и позволяя предотвращать развитие аварийных ситуаций на самых ранних, докритических стадиях.

Энергетическая безопасность склада обеспечивается многоуровневой системой резервирования питания. Помимо традиционных дизельных генераторов, современные комплексы оснащаются литий-железо-фосфатными аккумуляторными батареями повышенной емкости, способными поддерживать работу критически важных систем в течение нескольких часов.

Инновационным решением становится интеграция локальных источников возобновляемой энергии – солнечных панелей на крышах складов и систем рекуперации энергии, преобразующих кинетическую энергию движущейся техники в электрическую. Особое внимание уделяется архитектуре энергораспределения – кольцевая схема с автоматическими переключателями позволяет изолировать поврежденные участки сети без прекращения питания всего комплекса.

Противопожарная защита современных складов представляет собой сложный инженерный комплекс, сочетающий несколько уровней защиты. Аспирационные системы сверхраннего обнаружения дыма способны выявить возгорание на стадии тления, когда температура еще не достигла критических значений.

Автоматизированные системы пожаротушения нового поколения используют адресное воздействие, подавая огнетушащее вещество точно в зону возгорания, что минимизирует ущерб от самого процесса тушения. Инновационные термочувствительные покрытия на металлических конструкциях создают защитный барьер, замедляющий распространение огня. Архитектура склада разделена на изолированные противопожарные отсеки с автоматическими огнестойкими дверями, ограничивающими распространение возможного возгорания.

Особое место в системе безопасности занимают технологии предиктивной аналитики. На основе анализа больших массивов телеметрических данных и исторических показателей, системы с искусственным интеллектом способны прогнозировать возможные отказы оборудования задолго до их возникновения. Цифровые двойники складских комплексов позволяют в виртуальной среде моделировать различные аварийные сценарии, отрабатывая

оптимальные алгоритмы реагирования без риска для реального оборудования. Эти технологии дополняются системами автоматического технического обслуживания, которые по заранее определенным алгоритмам проводят профилактику критически важных узлов и агрегатов.

Реализация столь комплексного подхода требует не только современных технологических решений, но и тщательно проработанных организационных мер. Персонал проходит регулярное обучение действиям в нештатных ситуациях, при этом особый акцент делается на взаимодействии с автоматизированными системами безопасности. Разрабатываются и регулярно тестируются планы эвакуации и аварийного реагирования, адаптированные к специфике полностью автоматизированных складов. Все системы безопасности проходят обязательную сертификацию и регулярные проверки с привлечением независимых экспертов.

Принимая комплексные меры складские комплексы могут быть надежно защищены от техногенных катастроф при условии реализации всеобъемлющего подхода, сочетающего передовые технологии мониторинга, многоуровневые системы защиты, интеллектуальные системы прогнозирования и хорошо подготовленный персонал.

Такой комплексный подход позволяет снизить вероятность возникновения катастрофических ситуаций до минимально возможного уровня, обеспечивая бесперебойную и безопасную работу этих критически важных элементов современной логистической инфраструктуры.

Заключение

Автоматизированные склады, ставшие технологическим фундаментом современной логистики, сегодня переживают период стремительной трансформации. Переход к полностью автономным системам управления, сопровождающийся масштабной цифровизацией всех процессов, создает принципиально новые вызовы в области безопасности. Проведенное исследование наглядно демонстрирует, что традиционные подходы к защите складских комплексов уже не соответствуют современным угрозам, требующим комплексных интегрированных решений.

Основной вывод работы заключается в том, что безопасность автоматизированных складов должна рассматриваться как единая киберфизическая система, где цифровые и физические компоненты взаимосвязаны и взаимозависимы. Киберугрозы, представляющие наибольшую опасность, эволюционируют вместе с технологиями – от банальных вирусных атак до изощренных методов воздействия на промышленные контроллеры и системы позиционирования автономной техники. При этом физическая безопасность усложняется за счет масштабов современных складских комплексов и минимизации человеческого присутствия, а техногенные риски приобретают каскадный характер, когда локальный сбой может парализовать работу всего предприятия.

Перспективным и высокоэффективным направлением развития современных систем безопасности представляется создание интеллектуальных платформ нового поколения, в основе которых лежат передовые технологии искусственного интеллекта, машинного обучения и предиктивной аналитики. В отличие от традиционных систем, которые ограничиваются пассивным мониторингом и реагированием на уже произошедшие инциденты, такие решения способны заблаговременно выявлять потенциальные угрозы за счет комплексного анализа огромных массивов данных в режиме реального времени.

Современные интеллектуальные системы безопасности могут обрабатывать тысячи параметров работы оборудования, включая температурные режимы, вибрации, энергопотребление, сетевую активность и другие критические показатели. Благодаря алгоритмам машинного обучения система не только фиксирует отклонения от нормы, но и выявляет сложные корреляции, которые могут указывать на скрытые угрозы, такие как попытки кибератак, технические неисправности или несанкционированные действия персонала.

Особую важность приобретает возможность прогнозирования аварийных ситуаций до их возникновения. Например, предиктивная аналитика позволяет на основе исторических данных и текущих показателей спрогнозировать вероятность выхода оборудования из строя

или обнаружить признаки подготовки внештатной ситуации. Это дает возможность принять превентивные меры, минимизировать риски и избежать значительных финансовых потерь.

Ключевым аспектом успешного внедрения таких систем является разработка стандартизированных решений, обеспечивающих высокую степень совместимости между различными компонентами безопасности. Современные логистические комплексы включают множество подсистем – видеонаблюдение, контроль доступа, противопожарную сигнализацию, киберзащиту и другие. Интеграция этих компонентов в единую платформу позволяет создать целостное защищенное пространство, в котором все элементы взаимодействуют между собой, обмениваются данными и оперативно реагируют на любые аномалии.

Практическая значимость исследования заключается в том, что предложенные подходы к организации безопасности могут быть адаптированы как для строящихся, так и для уже эксплуатируемых складских комплексов.

Внедрение интегрированных систем защиты позволит значительно снизить операционные риски, минимизировать финансовые потери от простоев и обеспечить бесперебойность критически важных логистических процессов. В условиях растущей конкуренции на рынке складской недвижимости и логистических услуг, безопасность становится не просто обязательным требованием, а ключевым конкурентным преимуществом, позволяющим компаниям гарантировать клиентам надежность и стабильность поставок.

Таким образом, дальнейшее развитие автономных складов неизбежно потребует пересмотра существующих парадигм безопасности. Только комплексный подход, объединяющий передовые технологические решения, продуманные организационные меры и постоянный мониторинг новых угроз, позволит создать по-настоящему устойчивую и надежную систему защиты логистических комплексов будущего. Представленные в исследовании концепции и методики открывают новые возможности для построения таких систем, обеспечивающих не только сохранность материальных ценностей, но и непрерывность бизнес-процессов в условиях цифровой экономики.

Список использованных источников

1 Хакеры взломали систему управления холодильным оборудованием агрохаба [Электронный ресурс] // URL: https://dzen.ru/a/YiizMYLMhTzGaZiM?ysclid=mc7e8ystb4345775444

2 Пожар на складе Wildberries [Электронный ресурс] // URL: https://ren.tv/longread/1180832-pozhar-na-sklade-wildberries-nazvan-samym-strashnym-v-istorii-biznesa-rf

3 Маликова, Т. Е. Склады и складская логистика: учебное пособие для вузов / Т. Е. Маликова. – Москва: Издательство Юрайт, 2023. – 157 с.

4 Дыбская, В. В. Логистика складирования : учебник / В. В. Дыбская. – Москва: ИНФРА-М, 2023. – 559 с.

5 Дыбская, В. В. Проектирование системы распределения в логистике: монография / В.В. Дыбская. – Москва: ИНФРА-М, 2024. – 235 с.

6 Логистика и управление цепями поставок на транспорте: учебник для вузов / И. В. Карапетянц [и др.]; под редакцией И. В. Карапетянц, Е. И. Павловой. – 2-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2024. – 410 с.

7 Тяпухин, А. П. Логистика в 2 ч. Часть 1: учебник для вузов / А. П. Тяпухин. – 3-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2024. – 386 с.

8 Тяпухин, А. П. Логистика в 2 ч. Часть 2: учебник для вузов / А. П. Тяпухин. – 3-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2024. – 223 с.

9 Бочкарев, А. А. Логистика городских транспортных систем: учебное пособие для вузов / А. А. Бочкарев, П. А. Бочкарев. – 3-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2024. – 162 с.

10 Григорьев, М. Н. Коммерческая логистика: теория и практика: учебник для вузов / М. Н. Григорьев, В. В. Ткач, С. А. Уваров. – 3-е изд.,

РАБОЧИЙ ГРАФИК ПРОВЕДЕНИЯ

учебной практики по получению навыков исследовательской работы

Студент: Соколов Михаил Алексеевич

Направление подготовки: 23.03.01 / Технология транспортных процессов

Кафедра: Кафедра транспортных процессов и технологий

Группа: БТТ-24-ЭУ1

Руководитель практики от ОО: Карсаков Кирилл Борисович, Ассистент

С правилами трудового распорядка ознакомлен _____ Соколов М. А.
(подпись обучающегося)

Этапы НИР

Этап практики	Виды работ	Содержание выполняемых работ	Срок выполнения	Отметка о выполнении
Подготовительный	Организационное собрание	Участие в организационном собрании; беседа с сотрудниками РИАЦ либо кафедры. Коммуникации с руководителем практики для обсуждения содержания, цели, задач практики, выбора направления исследования	с 24.02.2025 по 25.02.2025	
Анализ литературных источников	Осуществление поиска источников литературы как в книжном, так и в электронном форматах	Посещение городской библиотеки № 13, ознакомление с электронными ресурсами	с 25.02.2025 по 10.03.2025	
Сбор данных	Был составлен список подходящей литературы, с последующим ознакомлением	Библиотека № 13, онлайн-ресурсы	с 10.03.2025 по 12.04.2025	
Обработка и интерпретация данных	Составление научной статьи, опираясь на источники литературы	Были составлены план действий и начато конспектирование научного исследования	с 12.04.2025 по 14.05.2025	

Написание отчёта	———	Написание отчёта	с 14.05.2025 по 24.06.2025	
Подготовка к защите отчёта	———	Подготовка и оформление отчёта по практике	25.06.2025	
Защита отчёта	———	Защита отчёта по практике	28.06.2025	

Руководитель практики от ОО:
Ассистент _____ Карсаков К. Б.
(подпись)

Согласовано:
Директор ИШ _____ Кузнецов П.А.
(подпись)