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

Научно-исследовательская практика

Защищенность современных автономных складов

Выполнил студент группы:
БТТ-24-ЭУ1 Соколов М.А

Руководитель: ассистент
Карсаков К.Б.

Владивосток 2025

Актуальность темы

Автоматизированные склады стали ключевым звеном глобальных цепочек поставок, но их зависимость от цифровых технологий создает новые уязвимости. Кибератаки, физические проникновения и техногенные аварии могут парализовать работу склада, что приведет к миллионным убыткам. Традиционные методы защиты уже не справляются с этими вызовами, что делает разработку новых решений критически важной для отрасли.

Рисунок 1 – полностью автоматизированный склад

Цель исследования

Целью работы является создание интегрированной системы безопасности, которая объединит физическую защиту, кибербезопасность и интеллектуальный мониторинг в единый комплекс. Система должна минимизировать человеческое вмешательство, автоматически выявлять угрозы и оперативно на них реагировать, обеспечивая бесперебойную работу склада даже в условиях внешних атак или внутренних сбоев.

Современные угрозы

Автономные склады сталкиваются с тремя основными типами угроз. Кибератаки на системы управления могут привести к остановке работы или порче товаров. Физические проникновения усложняются из-за минимального присутствия персонала. Техногенные риски, такие как пожары или сбои энергоснабжения, способны вызвать каскадные аварии. Эти угрозы требуют комплексного подхода к безопасности.

Кибербезопасность

Кибератаки становятся все более изощренными: от взлома систем управления до внедрения вредоносного ПО. Примером является атака на агрохаб «Селятино», где хакеры попытались изменить температурный режим хранения. Для защиты необходимо внедрять многоуровневую аутентификацию, сегментировать сети и использовать машинное обучение для выявления аномалий в режиме реального времени.

Рисунок 2 – логистический хаб «Селятино»

Физическая безопасность

Ограниченное присутствие персонала делает склады уязвимыми для физических проникновений. Злоумышленники используют подделку биометрии, повреждение датчиков или провокацию ложных срабатываний систем. Современные решения включают интеллектуальное видеонаблюдение с распознаванием аномалий, биометрический контроль доступа и дублирование критических систем для предотвращения саботажа.

Рисунок 3 – Биометрический контроль доступа

Техногенные риски

Пожары, сбои электроснабжения и поломки оборудования могут парализовать работу склада. Например, возгорание на складе в Шушарах привело к убыткам в миллиарды рублей. Для снижения рисков необходимы системы предиктивной аналитики, резервные источники энергии и автоматизированные противопожарные комплексы, способные локализовать возгорание без участия человека.

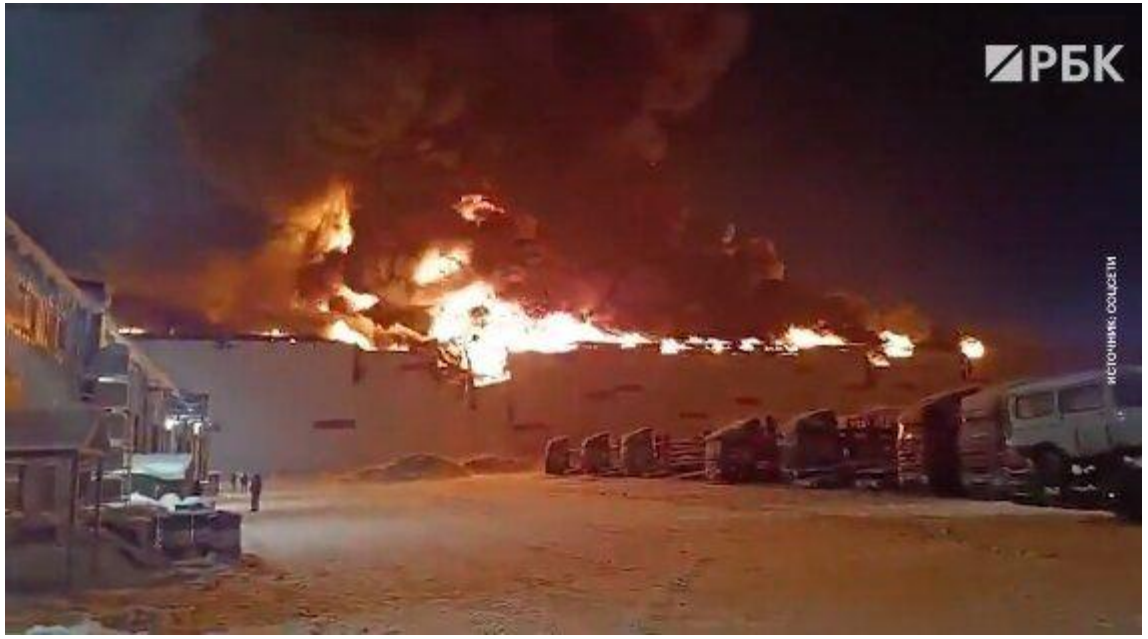

Рисунок 4 – Пожар на складе Wildberries

Интеллектуальный мониторинг

Искусственный интеллект и машинное обучение позволяют прогнозировать угрозы до их возникновения. Системы анализируют данные с датчиков, выявляют аномалии и автоматически принимают меры. Например, цифровые двойники складов помогают моделировать аварийные сценарии и разрабатывать превентивные меры, снижая вероятность реальных инцидентов.

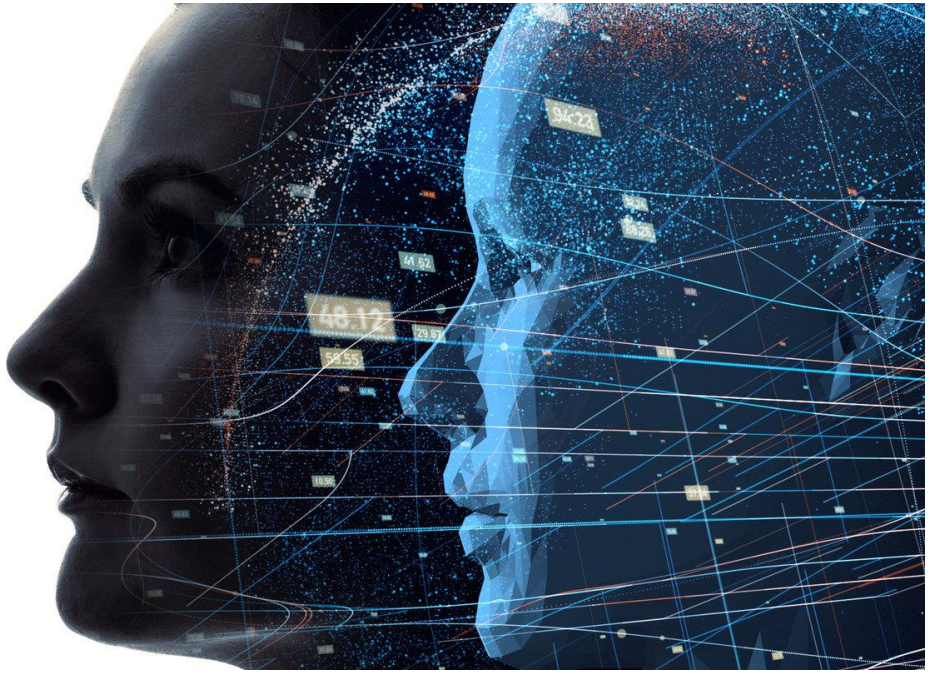

Рисунок 5 – Цифровые двойники

Практическая значимость

Внедрение интегрированной системы безопасности повысит отказоустойчивость складов и сократит финансовые потери. Решения могут быть адаптированы под существующую инфраструктуру, обеспечивая защиту без масштабной реконструкции. Это даст компаниям конкурентное преимущество и снизит риски в условиях растущих киберугроз и техногенных вызовов.

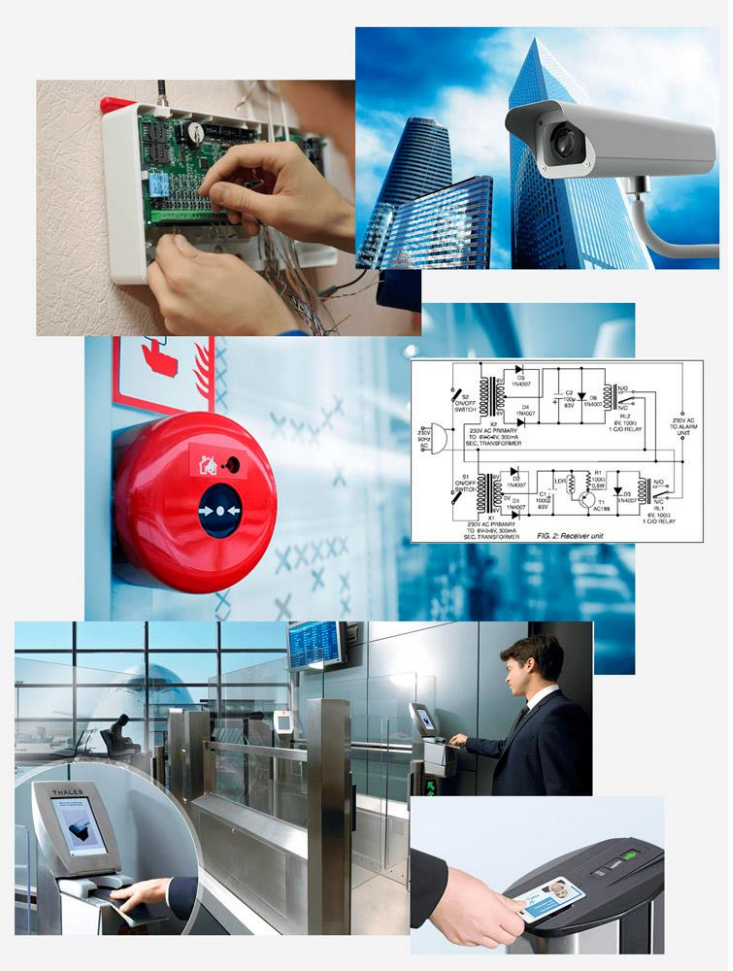

Рисунок 6 – Интегрированная система безопасности

Заключение

Автоматизированные склады будущего требуют принципиально новых подходов к безопасности. Интегрированная система на основе ИИ, объединяющая физическую и киберзащиту, способна обеспечить надежность и бесперебойность логистических процессов. Дальнейшие исследования должны быть направлены на стандартизацию таких решений и их внедрение в отраслевые практики.