4. Бобина М. А., Волков С. К. Сравнительный анализ алгоритмов распознавания лиц в условиях неидеального освещения // Информационные технологии и вычислительные системы. 2023. № 2. С. 12–24.

5. Шаров В. И., Новикова Т. П. Применение библиотеки OpenCV для задач компьютерного зрения в образовательных проектах // Современные информационные технологии и ИТ-образование. 2022. Т. 18, № 1. С. 120–129.

6. Документация библиотеки OpenCV. URL: https://docs.opencv.org/4.x/ (дата обращения: 15.12.2025).

7. 25 Object Detection with HAAR Cascade Classifiers. URL: https://www.youtube.com/watch?v=kThRJyQCW-8 (дата обращения: 15.12.2025).

8. Continuous Human Action Recognition Using Depth-MHI-HOG and a Spotter Model. URL: https://www.mdpi.com/1424-8220/15/3/5197 (дата обращения: 15.12.2025).

9. Deep Learning Vs Machine Learning. URL: https://k21academy.com/ai-ml/dl-vs-ml/ (дата обращения: 15.12.2025).

ОСОБЕННОСТИ МУЛЬТИМЕДИЙНЫХ ПАРКОВ КАК ОБЪЕКТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Чикарь Л. А., Мозговенко А. А.

ФГБОУ ВО «Мелитопольский государственный университет», Мелитополь, e-mail: ya@amozgovenko.ru

Задачи исследования:

1. Определить понятие «информационная безопасность».

2. Осуществить анализ существующих типов угроз.

3. Выявить интересы субъектов информационных отношений.

4. Провести анализ мер защиты.

Материалы и методы исследования

Исследования и публикации в области информационной безопасности мультимедийных парков:

1. Научная статья Ирины Владимировны Топчий «Мультимедийные технологии в современном музее как инструмент привлечения посетителей (на примере музея-заповедника «Аркаим»)» (журнал «Знак: проблемное поле медиаобразования», 2024). В статье рассмотрены возможности использования мультимедийных технологий в пространстве музея, а также классификации таких технологий.

2. Исследование Т. В. Румянцевой «Роль медиапроектов при продвижении музея» (2024). Исследователь отмечает, что оригинальный медиа контент, основанный на уникальной экспозиции, может быть представлен в формате виртуального пространства музея в виде видеоролика или трейлера для популяризации его деятельности [2].

Основная цель – создать защиту информации и поддерживающей её инфраструктуры от случайных или преднамеренных воздействий, которые могут нанести ущерб владельцам или пользователям информации.

Результаты исследования и их обсуждение

Рассмотрим мультимедийный парк как объект информационной безопасности – обеспечение конфиденциальности, целостности и доступности информации в информационных системах, связанных с использованием мультимедийных технологий. Это связано с тем, что мультимедийные данные (изображение, видео, аудио) подвергаются угрозам, и необходимо минимизировать риски, прогнозировать возможные негативные воздействия и предотвращать их.

Виды целей информационной безопасности для мультимедийных парков:

1. Конфиденциальность – доступ к информации только у лиц, имеющих на это полномочия.

2. Целостность – блокировка несанкционированного изменения информации.

3. Доступность – возможность получить требуемую информационную услугу за приемлемое время.

4. Подлинность – полнота и общая точность информации.

5. Неотказуемость – возможность определить источник или авторство информации [1].

Эти цели важны, так как информационные системы создаются для получения определённых информационных услуг, и, если предоставить эти услуги пользователям становится невозможно, это наносит ущерб [3].

Все эти элементы связаны в единую сеть, обеспечивающую бесперебойное функционирование контента и сервисов, и именно эта взаимосвязанность определяет особую уязвимость подобной среды. Любое нарушение в одном из сегментов инфраструктуры может повлечь за собой цепную реакцию сбоев, затронуть критические активы и повлиять на доступность и целостность информации.

С точки зрения информационной безопасности мультимедийные парки относятся к категории объектов с повышенной степенью риска. Это объясняется их публичностью, открытым доступом для большого количества пользователей и разнообразием подключаемых устройств, зачастую использующих стандартные беспроводные интерфейсы и протоколы связи. Высокая плотность цифрового оборудования и использование множества каналов передачи данных (локальные сети, Wi-Fi, Bluetooth, NFC, IT-протоколы) создают широкое поле для потенциальных киберугроз. При этом специфика работы подобных учреждений требует постоянного взаимодействия с внешними источниками информации – облачными платформами, сервисами обновления контента, платёжными шлюзами и базами данных партнёров, что дополнительно увеличивает количество точек возможного воздействия.

Мультимедийные парки одновременно выполняют функции культурно-просветительско-

го учреждения, технологической лаборатории и коммерческого предприятия [7].

Особенности мультимедийных парков как объекта информационной безопасности: Отдельного внимания заслуживает внедрение технологий машинного обучения и искусственного интеллекта в обеспечение информационной безопасности [8]. Алгоритмы анализа поведенческих паттернов позволяют определять аномалии в работе систем и действий пользователей, предсказывать возможные инциденты и минимизировать человеческий фактор при принятии решений. В условиях мультимедийного парка такие технологии позволяют обнаруживать подозрительные действия в реальном времени – например, несанкционированное подключение к локальной сети, попытки доступа к серверу контента или изменения в структуре базы данных посетителей.

Ключевые угрозы информационной безопасности

Атаки на системы управления технологическими процессами (SCADA/OT): взлом систем управления движением, освещением, вентиляцией или механикой аттракциона может привести к созданию опасных ситуаций, причинению вреда здоровью.

Программы-вымогатели (Ransomware): шифрование данных билетных систем, баз данных персонала и гостей, систем управления очередью с целью получения выкупа. Блокировка систем в пиковые часы может парализовать работу всего парка.

Утечки персональных и биометрических данных: кража баз данных посетителей, включая фотографии, платежную информацию, данные о местоположении. Продажа таких данных на черном рынке или использование для целевого фишинга.

1. Атаки типа «отказ в обслуживании» (DDoS): направлены на онлайн-билетные кассы, мобильное приложение парка или внутренние сервисы, что приводит к хаосу на входе и финансовым потерям [6].

2. Компрометация публичных сетей Wi-Fi: организация «зловредных» точек доступа, перехват трафика гостей для кражи учетных данных или данных банковских карт.

3. Физический доступ к оборудованию: незащищенные коммутационные шкафы, медиаплееры или панели управления могут стать точкой входа в сеть для злоумышленника, действующего под видом посетителя.

4. Непреднамеренные воздействия – ошибки пользователя, сбой технических и программных средств информационных систем, природные явления, которые могут привести к искажению, уничтожению, копированию информации.

Для обеспечения информационной безопасности в мультимедийных парках необходимо принимать следующие мары:

1. Технические меры – создание безопасных каналов связи, защита серверов, обеспечение безопасности внешних носителей и рабочих мест пользователей.

2. Организационные меры – подготовка сотрудников, обучение их типовым действиям, необходимым для соблюдения информационной безопасности. Например, проведение тренингов по информационной безопасности, разработка инструкций для сотрудников разных отделов, где поясняются их зоны ответственности и содержатся правила соблюдения режима безопасности. [5]

3. Криптографические методы – шифрование отдельных сообщений и информационного трафика, криптографическая аутентификация объектов сети.

4. Защита протоколов – например, защита физического уровня, обеспечивающего электрические, функциональные и процедурные средства установления, поддержания и разъединения физического соединения, с использованием механизма шифрования.

5. Сегментация сетей (Zero Trust Architecture): обязательное разделение сетей OT, IT, IT и гостевого Wi-Fi с помощью межсетевых экранов следующего поколения (NGFW). Принцип «никому не доверяй, проверяй каждый запрос».

6. Всеобъемлющий мониторинг и SIEM-системы: внедрение систем безопасности для операционных технологий (OT Security), сбор и корреляция логов со всех компонентов (датчики, медиасерверы, системы контроля доступа) в едином центре управления информационной безопасностью (SOC).

7. Защита данных и соблюдение нормативных требований: строгое применение принципов Privacy by Design, шифрование данных на rest и in transit, внедрение DLP-систем для предотвращения утечек, регулярные аудиты на соответствие 152-ФЗ и отраслевым стандартам.

8. Регулярное обучение и повышение осведомленности персонала: обязательные кибертренинги для всех сотрудников, от администраторов до аниматоров, с акцентом на фишинг и социальную инженерию. Разработка clear desk и clear screen политик.

9. Инцидент-менеджмент и аварийное восстановление: разработка детальных планов реагирования на инциденты информационной безопасности (кибератака, утечка данных), регулярные учения, наличие актуальных и изолированных резервных копий критических систем.

10. Физическая безопасность информационных технологий -инфраструктуры: ограничение доступа в серверные комнаты и технические помещения, использование средств контроля физического доступа, защита конечных точек (USB-порты и т.д.).

Важно учитывать, что универсальных методов защиты не существует, успех при построении

механизмов безопасности для реальной системы зависит от её индивидуальных особенностей.

Заключение

Мультимедийный парк – это не просто место развлечений, а высокотехнологичный критический объект, где цифровая и физическая безопасность неразделимы. Традиционные подходы к информационной безопасности здесь недостаточны. Требуется специализированная стратегия, учитывающая гибридную природу инфраструктуры, высочайшие требования к доступности и целостности, а также повышенные риски, связанные с обработкой биометрических данных. Упреждающие инвестиции в построение адаптивной, многослойной системы защиты являются не статьей расходов, а ключевым условием устойчивого бизнеса, сохранения репутации и, что самое важное, безопасности тысяч посетителей, доверяющих парку свои данные и досуг.

Список литературы

1. Вострецова Е. В. Основы информационной безопасности: учебное пособие, 2019. 208 с.

2. Буданов Д. Нюансы организации информационной безопасности в музеях // Системы безопасности». 2025. № 2.

3. Богданов А. В., Малыгин И. Г., Синещук Ю. И. Неформальная модель нарушителя безопасности объектов культуры // Вестник Санкт-Петербургского университета ГПС МЧС России. 2013. № 3. С. 109–113. URL: vestnik.igps.ru (дата обращения: 18.10.2025).

4. Корчагин С. И., Павлов В. Г., Бутов А. Н., Ткаченко Д. Г. Подходы к созданию систем обеспечения безопасности особо важных объектов // Системы безопасности. 2010. № 4.

5. Семкин С. Н., Беляков Э. В., Гребенев С. В., Козачок В. И. Основы организационного обеспечения информационной безопасности объектов информатизации: учеб. пособие. М.: Гелиос АРВ, 2005.

6. Климов С. М. Методы и модели противодействия компьютерным атакам. Люберцы: КАТАЛИСТ, 2008.

7. Пресс-конференция о работе мультимедийных исторических парков «Россия – моя история» [Электронный ресурс]. URL: http://pressmia.ru/pressclub/20171213/951788008.html (дата обращения: 18.10.2025).

8. Технологии интеллектуального музея нуждаются в этих 7 решениях Интернета вещей // Умный турист. 2022, 27 июня.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЯ ДЛЯ ПРОГНОЗИРОВАНИЯ ОБЪЁМА ВЫПУСКА ПРОДУКЦИИ ПРЕДПРИЯТИЯ

Шипилов Д. В., Мозговенко А. А.

ФГБОУ ВО «Мелитопольский государственный университет», Мелитополь, e-mail: ya@amozgovenko.ru

Цель исследования – разработать программное обеспечение на C#, обеспечивающее достоверное прогнозирование объёма выпуска продукции с учётом исторических данных, текущих заказов и производственных ограничений.

Задачи исследования:

1. Проанализировать существующие методы прогнозирования производственных показателей и выбрать оптимальные для реализации.

2. Определить требования к функциональности и интерфейсу ПО с учётом потребностей производственных менеджеров.

3. Разработать архитектуру приложения с модульной структурой (ввод данных, расчёт, визуализация, экспорт).

4. Реализовать алгоритмы обработки временных рядов и статистического анализа на C#.

5. Обеспечить интеграцию с типовыми ERP системами через API или CSV импорт/экспорт.

6. Протестировать ПО на реальных производственных данных и оценить точность прогнозов.

Материалы и методы исследования

Современные исследования в области прогнозирования производственных объёмов фокусируются на:

– Машинном обучении. Публикации 2023–2025 гг. демонстрируют эффективность нейронных сетей (LSTM, GRU) для анализа временных рядов производства. Однако их внедрение требует больших объёмов данных и вычислительных ресурсов.

– Классических статистических методах. ARIMA, экспоненциальное сглаживание и регрессионный анализ остаются актуальными для предприятий с ограниченной историей данных.

– Интеграции с IoT. Исследования подчёркивают важность учёта данных с датчиков оборудования для корректировки прогнозов в реальном времени.

– Облачных решениях. Появление SaaS-платформ для производственного планирования (например, Oracle SCM, SAP IBP) задаёт стандарты юзабилити и масштабируемости.

– Визуализации данных. Современные работы акцентируют необходимость интерактивных дашбордов с KPI и сценарным анализом.

Основная цель – создать гибкое, масштабируемое ПО на C#, сочетающее проверенные статистические методы и элементы машинного обучения для прогнозирования объёмов производства.

Результаты исследования и их обсуждение

Для разработки данного программного обеспечения был использован язык программирования C#. Были задействованы следующие библиотеки (рис. 1):

System;
System.Collections.Generic;
System.ComponentModel;
System.Data;
System.Drawing;