Иванов Егор Сергеевич
Студентка Института инженерных и цифровых технологий НИУ «БелГУ»
г. Белгород
Ivanov Egor Sergeevich
Student, Institute of Engineering and Digital Technologies, Belgorod State University
Belgorod

ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ПДн В ДЕЯТЕЛЬНОСТИ АКВАПАРКА

REQUIREMENTS FOR ENSURING INFORMATION SECURITY WHEN WORKING WITH PERSONAL INFORMATION IN THE ACTIVITIES OF A WATER PARK

Аннотация: В статье рассматриваются актуальные проблемы защиты информации в гостиничных телекоммуникационных системах, представляющих собой сложные гетерогенные сети, объединяющие PMS-серверы, платёжные терминалы, Wi-Fi-инфраструктуру, VoIP-оборудование и устройства интернета вещей в «умных» номерах. Показано, что цифровая трансформация индустрии гостеприимства приводит к расширению векторов атак и увеличению поверхности уязвимости, что требует пересмотра традиционных подходов к сетевой безопасности.

Ключевые слова: аквапарк, персональные данные, информационная безопасность

Abstract: This article examines current information security challenges in hotel telecommunications systems, which are complex heterogeneous networks that integrate PMS servers, payment terminals, Wi-Fi infrastructure, VoIP equipment, and IoT devices in smart rooms. It is shown that the digital transformation of the hospitality industry is leading to an expansion of attack vectors and a larger vulnerability surface, necessitating a reconsideration of traditional approaches to network security.

Keywords: water park, personal data, information security

Современный аквапарк представляет собой не просто совокупность водных

аттракционов, а сложное, технологически насыщенное предприятие индустрии развлечений и гостеприимства. Современные информационные технологии являются фундаментом для слияния бизнес-процессов и технических систем. Это позволяет достичь эффективного управления предприятием. Его эффективное функционирование напрямую зависит от бесперебойной работы множества взаимосвязанных информационных и инженерных систем, объединенных в единую телекоммуникационную инфраструктуру.

Компьютерные сети являются основой информационной инфраструктуры любого современного предприятия, обеспечивая взаимодействие всех компонентов информационной системы. Предметная область проектирования охватывает анализ бизнес-процессов, технологических контуров и информационных потоков аквапарка как объекта информатизации.

Проектирование сети начинается с формулировки четких, измеримых и верифицируемых требований. Они являются основой для выбора архитектуры, технологий и оборудования. Требования делятся на функциональные (что должна делать сеть) и нефункциональные (какими качествами обладать).

– Функциональные требования

Сеть должна обеспечивать связность и доступность сервисов для всех категорий пользователей и систем:

1. для бизнес-приложений: гарантированный доступ к серверам 1С, CRM, биллинга с рабочих мест администрации, бухгалтерии, менеджеров. Доступ должен быть защищенным и быстрым (<100 мс ping);

2. для посетителей: предоставление изолированного гостевого Wi-Fi доступа в Интернет в зонах отдыха, кафе, лобби. Обязательна авторизация и фильтрация контента. Пропускная способность на пользователя – не менее 2 Мбит/с для комфортного серфинга.

3. для технологических систем: видеонаблюдение: резервированная полоса пропускания для передачи потоков с 20+ камер (до 20 Мбит/с на камеру) к серверам видеорегистрации.

СКУД и кассы: стабильный, низколатентный канал связи для турникетов,

билетных терминалов и сервера базы данных. Протоколы передачи должны обеспечивать целостность транзакций;

АСУ ТП: выделенный, логически изолированный сегмент сети для оборудования жизнеобеспечения. Требуется поддержка необходимых промышленных протоколов и гарантированная доставка команд управления.

– Нефункциональные требования

1. Производительность и масштабируемость: магистраль (ядро сети): скорость не менее 10 Гбит/с с возможностью масштабирования до 40/100 Гбит/с; доступ к серверам: порт не менее 1 Гбит/с, для СХД и критичных серверов – 10 Гбит/с; доступ пользователей: проводные порты – 1 Гбит/с, Wi-Fi – стандарт 802.11ax (Wi-Fi 6) для высокой плотности подключений; сеть должна допускать увеличение числа подключенных устройств на 30% без замены основной архитектуры. Архитектура сети должна позволять легко добавлять новые устройства и подсети.

2. Надежность и доступность: целевой показатель доступности для критичных систем (кассы, СКУД, АСУ ТП) – 99.9% (время простоя не более 8.8 часов в год); реализация отказоустойчивой архитектуры: стекирование коммутаторов доступа и ядра, резервирование линков с использованием технологий LACP или STP, резервирование источников питания. Надежность сети определяется ее способностью выполнять возложенные на нее функции в течение заданного промежутка времени в заданных условиях эксплуатации; аппаратное резервирование критичных сетевых устройств (маршрутизаторы, межсетевые экраны) в режиме Active/Standby или Active/Active.

3. Управляемость и обслуживаемость: централизованное управление всем сетевым оборудоваством с единой консоли. Поддержка протоколов SNMPv3, NetFlow/sFlow для мониторинга; возможность сегментации на уровне VLAN для разделения трафика; поддержка QoS (IEEE 802.1p/DSCP) для приоритизации голосового трафика (VoIP), видео с камер и транзакционных данных; легкость диагностики и устранения неисправностей благодаря внятной документации и

логированию событий.

4. Безопасность (базовый уровень): возможность изоляции гостевой сети, сети видеонаблюдения и АСУ ТП от основной корпоративной сети и защита от петель и штормов широковещательного трафика (Storm Control).

Обработка персональных данных (далее - ПДн) является неотъемлемой частью работы аквапарка. ПДн посетителей (взрослых и детей) и сотрудников обрабатываются в биллинговых системах, CRM, кадровых системах. Согласно Федеральному закону № 152-ФЗ, администрация аквапарка является оператором ПДн и обязана обеспечить их защиту. Проект сети должен закладывать соответствие этим требованиям на архитектурном уровне.

Принципы и организационные требования к телекоммуникационным системам: принцип законности и целесообразности: обработка ПДн должна быть легальной, а сеть должна технически препятствовать обработке данных сверх заявленных целей (напр., данные гостя не должны попадать в систему маркетинга без его согласия); принцип минимизации прав доступа: сетевая архитектура и системы контроля доступа должны обеспечивать предоставление пользователям и системам минимальных необходимых прав для доступа к ПДн. Например, администратор видеонаблюдения не должен иметь сетевой доступ к серверу 1С с финансовыми данными. Этот принцип является ключевым, так как «разграничение доступа к информационным ресурсам системы является одной из основных мер защиты информации»; обязательность выделения сегментов сети: ИСПДн должны быть размещены в выделенном, изолированном сегменте (VLAN), доступ к которому строго контролируется межсетевыми экранами. Физические серверы или виртуальные машины, обрабатывающие ПДн, должны находиться в этом сегменте.

Телекоммуникационные сети аквапарка должны обладать следующими техническими требованиями к защите ПДн при передаче и хранении информации:

1. Конфиденциальность при передаче: все соединения с веб-интерфейсами систем, обрабатывающих ПДн (CRM, панель администрирования), должны использовать защищенные протоколы; передача ПДн между сегментами

сети должна шифроваться с использованием VPN (IPsec) или защищенных протоколов прикладного уровня; беспроводные сети, через которые возможен доступ к ПДн, должны использовать стойкие протоколы шифрования.

2. Целостность и доступность: должны быть реализованы механизмы контроля целостности программной среды и данных .

3. Учет и протоколирование: все сетевые устройства и серверы ИСПДн должны вести детальные журналы событий безопасности. Журналы должны быть централизованно собраны на выделенный сервер (SIEM) с защитой от модификации; должны регистрироваться все успешные и неуспешные попытки доступа к ПДн, изменения правил доступа, запуск критичных процессов. Регистрация и учет событий являются важной частью системы защиты информации, позволяющей обнаруживать нарушения политики безопасности. Таким образом, требования к защите ПДн не являются надстройкой, а интегрируются в фундамент проектирования сети, определяя ее сегментацию, политики межсетевого экранирования, требования к шифрованию и управлению доступом. Проведенный анализ и проектирование позволили сформировать современную сетевую среду аквапарка. Итоговая инфраструктура будет соответствовать техническим требованиям объекта, обеспечивая стабильную, безопасную и эффективную работу всех сетевых процессов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. **Баланов А. Н.** Защита информационных систем. Кибербезопасность : учебное пособие для СПО / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург : Лань, 2025. – 84 с. – ISBN 978-5-507-53004-5. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/464183.

2. **Баланов А. Н.** Комплексная информационная безопасность : учебное пособие для СПО / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург : Лань, 2025. – 284 с. – ISBN 978-5-507-52953-7. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/463001.

3. **Козырь, Н. С.** Анализ и оценка рисков информационной безопасности : учебник для среднего профессионального образования / Н. С.

Козырь, В. Н. Хализев. – Москва : Издательство Юрайт, 2025. – 157 с. – (Профессиональное образование). – ISBN 978-5-534-20645-6. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/581503.