Астраханский государственный университет им. В.Н.Татищева

Факультет цифровых технологий и кибербезопасности

Лабораторная работа №1. «Анализ и классификация информационных систем и знакомство со стандартами».

Кузургалиев Р.А. ДИФ-15 Ваиант 8

Синельщиков А.В.

21.09.2025

**СОДЕРЖАНИЕ РАБОТЫ**

**ВВЕДЕНИЕ**

**Цель:** Закрепить теоретические знания о классификации информационных систем, их жизненном цикле и роли архитектуры. Ознакомиться с основными стандартами, применяемыми при разработке и документировании ИС.

Лабораторная работа №1. «Анализ и классификация информационных систем и знакомство со стандартами».

Система бронирования авиабилетов предназначена для удобного поиска, бронирования, покупки авиабилетов.

**КЛАССИФИКАЦИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ**

1. **По сфере применения:**
   1. Классификация: Отраслевая система для сферы транспорта и логистики.
   2. Обоснование Система не является универсальной (как, например, бухгалтерская). Она создана специально для автоматизации ключевых бизнес-процессов в авиационной и туристической индустрии: продажа мест, управление пассажиропотоком, оказание сопутствующих услуг.
2. **По архитектуре:**
   1. Классификация: Веб-ориентированная система, построенная по многоуровнев ой архитектуре, часто с использованием облачных технологий (SaaS).
   2. Обоснование: Веб-ориентированная модель выбрана, потому что пользователи работают через удобный интерфейс, а обработка и хранение данных происходят на сервере. Облачный подход (SaaS) обоснован тем, что компания не хочет поддерживать собственную инфраструктуру, а предпочитает гибкость, масштабируемость и доступ из любой точки мира.
3. **По степени автоматизации:**
   1. Классификация: Автоматизированная информационная система.
   2. Обоснование: Система выполняет огромный объем работы автоматически (поиск, блокировка мест, генерация билетов), ключевые решения принимает человек-пользователь (выбор рейса, ввод персональных данных, подтверждение оплаты).
4. **По типу обработки данных:**
   1. Классификация: Транзакционная с элементами аналитики.
   2. Обоснование: Транзакционная обработка необходима для моментального учета операций (например, бронирование билетов или её отмены), что важно для оперативной работы с пользователями. Элементы аналитики добавлены для поддержки стратегических решений — например, анализ направлений или эффективности рейсов, что требует обработки накопленных данных.
5. **По масштабу:**
   1. Классификация: Корпоративная информационная система.
   2. Обоснование: Это крупная система, которая обслуживает все основные операционные процессы бизнеса авиакомпании или агрегатора: продажи, финансы (оплата), работу с клиентами (рассылка билетов, поддержка), логистику (управление местами).
6. **По функциональному назначению:**
   1. Классификация: Информационно-справочная система
   2. Обоснование: Основная и первичная функция системы — предоставление пользователям актуальной справочной информации по запросу.

**АНАЛИЗ СТАНДАРТОВ И НОРМАТИВНЫХ ДОКУМЕНТОВ**

Назначение: Онлайн-система для поиска рейсов, бронирования, оплаты и регистрации на рейс.

Особенности: Облачное развертывание (SaaS), обработка большого объема персональных и финансовых данных, интеграция с платежными шлюзами, GDS (глобальными дистрибьюторскими системами), email- и SMS-сервисами.

Регион применения: Россия.

**ISO/IEC 25010:2011 — Системы и программное обеспечение. Модель качества**

1. **Основные требования (пункты стандартов, которые должны быть учтены):**
   1. **Функциональная пригодность:** Система должна точно выполнять функции поиска рейсов, бронирования, оплаты, управления бронями и отправки уведомлений (Раздел 4.2.1 "Functional suitability").
   2. **Производительность:** Время отклика не более 2-3 секунд при пиковых нагрузках (например, запуск акционных тарифов, сезон бронирований) до нескольких тысяч одновременных пользователей (Раздел 4.2.3 "Performance efficiency").
   3. **Безопасность:** Защита финансовых транзакций и персональных данных пассажиров (PII) от несанкционированного доступа и мошенничества (Раздел 4.2.5 "Security").
   4. **Удобство использования:** Интуитивно понятный интерфейс для конечных пользователей, позволяющий быстро найти и забронировать билет (Раздел 4.2.7 "Usability").
2. **Что необходимо сделать (учесть) при разработке:**
   1. **Функциональность:** Разработать и протестировать модули поиска (интеграция с GDS API), бронирования (блокировка мест), оплаты (интеграция с платежными шлюзами), личного кабинета и админ-панели.
   2. **Производительность:** Провести стресс-тестирование и нагрузочное тестирование (например, с помощью k6 или JMeter) сценариев поиска рейсов и процесса оплаты под высокой нагрузкой.
   3. **Безопасность:** Внедрить PCI DSS-совместимые решения для оплаты, шифрование данных (TLS 1.3 для передачи, токенизация или AES для хранения платежных данных), защиту от мошеннических транзакций.
   4. **Удобство:** Провести юзабилити-тестирование с фокус-группами, внедрить адаптивный и отзывчивый (responsive) веб-дизайн.
3. **Обоснование (почему необходимо учесть):**
   1. **Функциональная пригодность:** Ядро бизнеса. Ошибки в поиске, бронировании или оплате приведут к прямым финансовым потерям и потере клиентов.
   2. **Производительность:** Медленный поиск или "зависание" при оплате приводят к брошенным корзинам и недовольству пользователей, особенно в условиях высокой конкуренции.
   3. **Безопасность:** Утечка данных банковских карт или паспортов нанесет катастрофический репутационный и финансовый ущерб.
   4. **Удобство использования:** Сложный процесс бронирования отпугнет менее технически подкованных пользователей.
4. **Требования, которые могут не учитываться (с обоснованием):**
   1. **Совместимость (Раздел 4.2.2 "Compatibility")** на уровне оборудования или специфического ПО.
   2. **Обоснование:** Система является SaaS-решением, работающим через стандартные веб-браузеры и мобильные приложения. Интеграция с внешними системами (GDS, платежки, email) осуществляется через общедоступные API.

**Федеральный закон РФ № 152-ФЗ "О персональных данных" (в ред. от 31.07.2023)**

Описание: Российский закон о защите ПДн

**Основные требования:**

* Локализация данных: Хранение ПДн граждан РФ на территории РФ (Статья 18, часть 5).
* Согласие на обработку: Получение явного согласия пользователя на обработку его ПДн (для целей, не связанных напрямую с исполнением договора, например, для маркетинга) (Статья 9).
* Минимизация данных: Сбор только необходимых для продажи авиабилета данных (Статья 5).
* Безопасность ПДн: Реализация мер по защите данных от несанкционированного доступа (Статья 19).

**Что необходимо сделать (учесть) при разработке:**

* Локализация: Выбрать облачного провайдера (например, Yandex Cloud) с дата-центрами в России для размещения серверов и баз данных с ПДн.
* Уведомление Документировать процесс обработки и подать уведомление через юриста.
* Минимизация Ограничить поля ввода (имя, email, телефон).

**Обоснование:**

* Локализация Данные россиян должны храниться в РФ для соблюдения закона. Провайдер с локальными серверами или гибридное решение предотвращает штрафы.
* Уведомление Регистрация в Роскомнадзоре — формальность, требующая описания целей обработки (ведение клиентской базы).
* Минимизация Сбор лишних данных запрещен. Ограничение полей ввода минимизирует риски и упрощает управление данными

**Требования, которые могут не учитываться (с обоснованием):**

* Обезличивание данных Статья 7 Обработка ПДн в форме, не позволяющей идентифицировать субъекта.
* Обоснование: CRM требует точной идентификации клиентов (имя, телефон) для продаж и общения, поэтому обезличивание противоречит ее назначению.
* Трансграничная передача данных Статья 12 Регулирование передачи ПДн за пределы РФ, если это не требуется.
* Обоснование Данные хранятся в РФ, а интеграция с сервисами ЕС (например, email) не предполагает передачу ПДн за пределы локализованной базы.

**ISO/IEC 27001:2013 — Информационная безопасность**

Описание: Стандарт управления системой информационной безопасности (СИБ).

**Основные требования:**

* Оценка рисков: Регулярная оценка рисков для информации (ПДн, финансовые данные) (Раздел 6.1.2).
* Управление доступом: Строгий контроль и разграничение прав доступа к данным и функциям системы (Приложение A.9).
* Инцидент-менеджмент: Процедуры по реагированию на инциденты безопасности (Приложение A.16).
* Криптография: Применение шифрования для защиты конфиденциальной информации (Приложение A.10).

**Что необходимо сделать (учесть) при разработке:**

* Риски: Провести анализ угроз и уязвимостей (например, по модели STRIDE или OWASP Top 10), уделив особое внимание уязвимостям инъекций (SQL), механизмам аутентификации и сессий.
* Контроль доступа: Внедрить ролевую модель (RBAC): Пользователь, Менеджер, Администратор. Пользователь имеет доступ только к своим бронированиям.
* Инциденты: Настроить систему мониторинга и оповещения (например, в Sentry, Grafana) о подозрительных действиях (множественные failed login attempts, массовые запросы на поиск).
* Криптография: Использовать современные алгоритмы шифрования (AES-256 для данных, bcrypt для хэшей паролей).

**Обоснование:**

* Система является привлекательной мишенью для злоумышленников (данные карт, ПДн). Внедрение процессов ISMS снижает риски и демонстрирует клиентам серьезный подход к безопасности.

**WCAG 2.1 — Руководство по доступности веб-контента**

**Описание:**Рекомендации для обеспечения доступности веб-интерфейсов для людей с ограниченными возможностями.

**Основные требования (Уровень AA):**

* Воспринимаемость: Альтернативные тексты для изображений, семантическая верстка (Принцип 1.3).
* Управляемость: Полная навигация и совершение заказа с помощью клавиатуры (Принцип 2.1).
* Контрастность: Достаточный коэффициент контрастности текста (4.5:1) (Критерий 1.4.3).

**Что необходимо сделать (учесть) при разработке:**

* Воспринимаемость: Добавить alt-тексты для логотипов и иконок, использовать семантические теги HTML5 (<header>, <nav>, <main>, <button>).
* Управляемость: Обеспечить четкую визуальную индикацию фокуса для всех интерактивных элементов, возможность заполнить все формы и нажать все кнопки с клавиатуры.
* Понятность: Четко маркировать все поля ввода, предоставлять понятные сообщения об ошибках (не просто "Ошибка", а "Номер карты введен неверно").
* Контрастность: Проверить и адаптировать цветовую схему (текст/фон) под требования контраста.

Обоснование:

* Соблюдение принципов доступности расширяет аудиторию пользователей, включая людей с ограниченными возможностями, и является требованием законодательства во многих странах, а также лучшей практикой.

**PCI DSS (Payment Card Industry Data Security Standard)**

Описание: Международный стандарт безопасности индустрии платежных карт.

**Основные требования:**

* Защита данных карт: Шифрование данных карт при передаче и хранении.
* Защита от уязвимостей: Регулярное тестирование безопасности систем и приложений.
* Контроль доступа: Строгое разграничение доступа к данным карт по принципу need-to-know.
* Политика безопасности: Реализация и соблюдение политик информационной безопасности.

**Что необходимо сделать (учесть) при разработке:**

* Не хранить данные карт: Использовать метод токенизации через интегрированного платежного провайдера (например, CloudPayments, YooKassa). Это самый надежный способ снизить область действия PCI DSS.
* Защита передачи: Использовать только защищенные протоколы (TLS) для передачи любых данных на платежную страницу.
* Регулярный аудит: Проводить регулярное сканирование на уязвимости (ASV scans) и тесты на проникновение.
* Контроль доступа: Реализовать RBAC, чтобы доступ к журналам транзакций и данным карт (даже токенизированным) имел только ограниченный круг персонала.

**Обоснование:**

* Прямая работа с данными платежных карт обязывает соблюдать PCI DSS. Несоблюдение стандарта ведет к огромным штрафам от платежных систем и потере возможности принимать карты к оплате.

**Список использованных стандартов и нормативных документов**

1. ISO/IEC 25010:2011 — "Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models".
2. Федеральный закон РФ № 152-ФЗ "О персональных данных" — в редакции от 31.07.2023.
3. PCI DSS — Payment Card Industry Data Security Standard. v4.0.
4. ISO/IEC 27001:2013 — "Information technology — Security techniques — Information security management systems — Requirements".
5. WCAG 2.1 — "Web Content Accessibility Guidelines 2.1".