ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное

учреждение высшего профессионального образования

Национальный исследовательский университет

«Высшая школа экономики»

Московский институт электроники и математики

Факультет прикладной математики

Кафедра «Компьютерная безопасность»

ОТЧЁТ

по курсовой работе по дисциплине«Основы информационной безопасности»

Выполнил студент группы СКБ 172

Попов Юрий Леонидович

Москва 2020

Введение

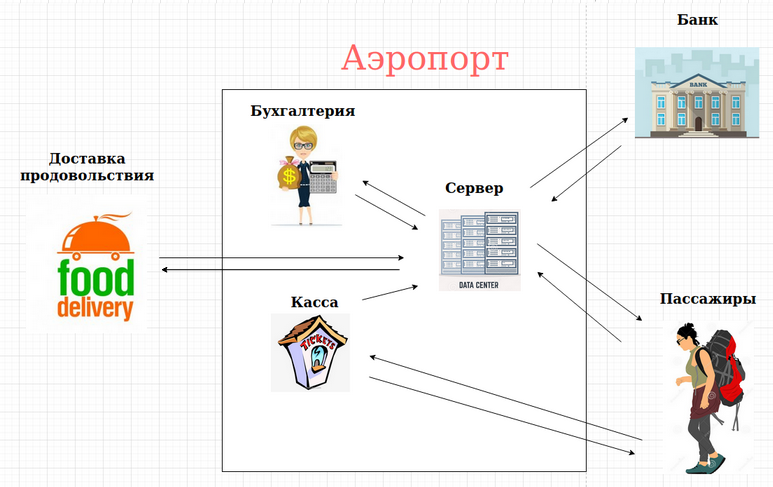
В качестве объекта информатизации был выбран аэропорт. Объект информатизации функционирует внутри одного здания.

Билеты продаются через кассу в здании аэропорта, а также на сайте аэропорта через личный кабинет. Данные о пассажирах, рейсах, цен на билеты хранятся на сервере.

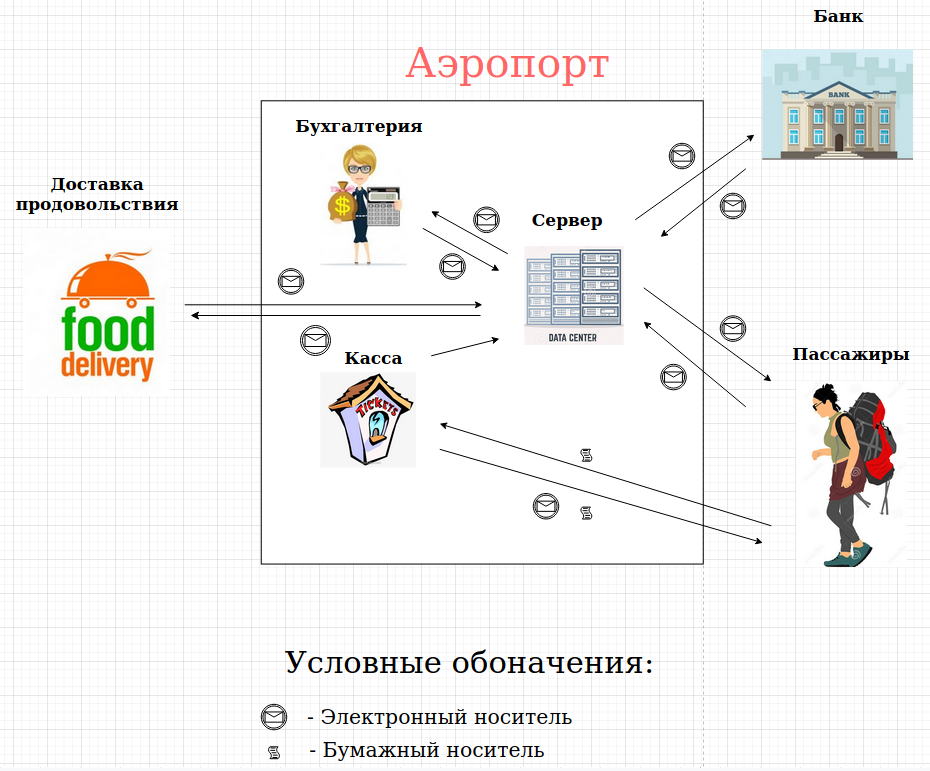
Денежные средства, поступающие от пассажиров учитываются в бухгалтерии, а затем отправляются в банк, с которым аэропорт взаимодействует через сервер. От сервера бане получает всю необходимую информацию, а затем загружает туда данные о транзакциях.

Также аэропорт заключает контракты на поставку продовольствия. Бухгалтерия на сервере размещает информацию о требованиях и пожеланиях о еде, а внешние поставщики передают на сервер коммерческие предложения

Объект информатизации — Аэропорт

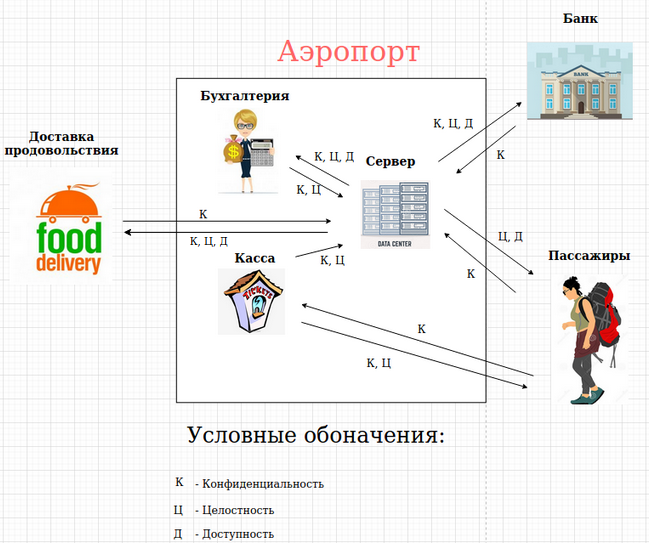


**Способы передачи данных**

**

Информация передаётся на бумажном носителе только при взаимодействии кассы с пассажиром. Например, персональные данные пассажира сканируются кассиром и печатается билет, который возвращается обратно пассажиру. Помимо бумажной копии, копия билета отправляется на почту пассажира.

**Свойства информации, которые необходимо обеспечить**



**Угрозы безопасности информации**

**УБИ1 =** [ террорист, работающий в сервере; свободный доступ во время рабочего дня; подрыв сервера, сервер, невозможность функционирования аэропорта]

(Д: Сервер → Бухгалтерия)

(Д: Сервер → Доставщики продовольствия)

**УБИ2 =** [системный администратор; неправильное конфигурирование сервера; доступ к конфиденциальным данным; утечка данных]

(К: Сервер → Бухгалтерия)

(К: Сервер → Доставщики продовольствия)

**УБИ3** = [уволенный сотрудник, устроившийся работать в доставку еды; низкая квалификация сотрудников аэропорта; разглашение содержания договоров; договоры; нарушение конфиденциальности договоров ](К: Доставка продовольствия→ Сервер)

**УБИ4 =** [искатель приключений, ищущий доступные данные в интернете; наличие веб- уязвимостей на сайте; ссылка, позволяющая получить доступ к данным на сервере; сервер; доступ до данных на сервере] (К: Сервер→ Болельщик)

**УБИ5 =** [хулиган; наличие веб- уязвимостей на сайте; применение различных векторов атак на сайт; сервер; доступ до данных на сервере] (К: Сервер→ Бухгалтерия)

**УБИ6 =** [разработчик ПО для бухгалтерии; наличие уязвимостей в проекте; доступ внешних лиц к данным в бухгалтерии; бухгалтерия; потеря или изменение данных]

(К: Бухгалтерия → Сервер)

(Ц: Бухгалтерия → Сервер)

**УБИ7 =** [кассир; плохое отношение к сотрудника; доступ к выдаваемой пассажирам информации; данные пассажиров; модификация данных] (Ц: Касса→ Пассажиры)

**УБИ8 = [** экстрамистические группировки; плохая репутация аэропорта; подрыв аэропорта; аэропорт; отказ в работе доступе аэропорта **]** (Д: Сервер→ Банк)

**УБИ9 = [** Агент007, устроившийся в доставку продовольствия; отсутствия контроля на вход; подрыв аэропорта; аэропорт; отказ в работе аэропорта **]** (Д: Сервер→ Пассажиры)

**УБИ10 = [** Завербованный кассир; свободный доступ к данным пассажира; модификация данных пассажиров; персональные данные пассажиров; потеря или изменения данных пассажиров**]**

(К, Ц: Касса→ Сервер)

**Формальные модели нарушителей**

| Нарушитель | Тип | Вид | Потенциал | Цель | Возможные способы реализации угроз |
| --- | --- | --- | --- | --- | --- |
| Террорист  (УБИ1) | Внутренний | Специальные службы иностранных государств | Высокий | Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики | Несанкционированный доступ и воздействия на каналы связи, тех. средства, машинные носители информации |
| Сис. Админ  (УБИ2) | Внутренний | Лица, обслуживающие инфраструктуру оператора | Базовый низкий | Непреднамеренные, неосторожные или неквалифицированные действия | Несанкционированный доступ и воздействия на каналы связи, тех. средства, машинные носители информации |
| Курьер  (УБИ3) | Внешний | Бывшие работники | Базовый низкий | Месть за ранее совершенные действия | Социальная инженерия |
| Искатель приключений  (УБИ4) | Внешний | Внешние субъекты (физические лица) | Базовый низкий | Любопытство или желание самореализации (подтверждение статуса) | Перехват информации по оптическому каналу |
| Хулиган  (УБИ5) | Внешний | Внешние субъекты (физические лица) | Базовый низкий | Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды | Несанкционированный доступ и социальная инженерия |
| Разработчик ПО(УБИ6) | Внешний | Разработчики, производители, поставщики программных, технических и программно-технических средств | Базовый повышенный | Непреднамеренные, неосторожные или неквалифицированные действия | Несанкционированный доступ и воздействия на каналы связи, тех. средства, машинные носители информации |
| Кассир  (УБИ7) | Внутренний | Пользователи информационной системы | Базовый низкий | Месть за ранее совершенные действия | Несанкционированный доступ и воздействия на каналы связи, тех. средства, машинные носители информации |
| Экстрамистические группировки  (УБИ8) | Внешний | Террористические, экстремистские группировки | Базовый повышенный | Дестабилизация деятельности органов государственной власти | Социальная инженерия |
| Агент007  (УБИ9) | Внешний | Специальные службы иностранных государств | Высокий | Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики | Перехват информации по оптическому каналу |
| Завербованный кассир  (УБИ10) | Внутренний | Пользователи информационной системы | Базовый низкий | Месть за ранее совершенные действия | Несанкционированный доступ и воздействия на каналы связи, тех. средства, машинные носители информации |

***Уровень проектной защищенности***

| **Структурно-функциональные характеристики информационной системы, условия её эксплуатации** | **Уровень защищенности** | | |
| --- | --- | --- | --- |
| **Высокий** | **Средний** | **Низкий** |
| 1. По структуре информационной системы:  локальная информационная система |  | + |  |
| 2. По используемым информационным технологиям:  системы с технологиями беспроводного доступа; |  |  | + |
| 3. По архитектуре информационной системы:   * системы на основе «тонкого клиента»; * файл-серверные системы; * центры обработки данных; * использование разных типов операционных систем; * использование выделенных каналов связи | + | +  + | +  + |
| 4. По наличию (отсутствию) взаимосвязей с иными информационными системами:  взаимодействующая с системами; |  |  | + |
| 5. По наличию (отсутствию) взаимосвязей (подключений) к сетям связи общего пользования:  подключённая через выделенную инфраструктуру (gov.ru или иную); |  | + |  |
| 6. По размещению технических средств:  расположенные в пределах одной контролируемой зоны; | + |  |  |
| 7. По режимам обработки информации в информационной системе:  многопользовательский; |  |  | + |
| 8. По режимам разграничения прав доступа:  с разграничением |  | + |  |
| 9. По режимам разделения функций по управлению информационной системой:  выделение рабочих мест для администрирования в отдельный домен; |  | + |  |
| 10. По подходам к сегментированию информационной системы:  с сегментированием |  | + |  |

**Итого:**

*«+» в высоком уровне: 2*

*«+» в среднем уровне: 7*

*«+» в низком уровне: 5*

*В высоком и среднем вместе: 9*

*Всего: 2 + 7 + 5 = 14*

*5/13 = 0.357 \* 100% = 35.7% > 10% =>*

Проектная защищенность **низкая**

***Актуальность угроз***

|  | **Уровень проектной защищенности** | **Потенциал нарушителя** | **Возможность реализации угрозы** | **Степень ущерба** | **Актуальность угрозы** |
| --- | --- | --- | --- | --- | --- |
| **УБИ1** | Н | В | В | В | А |
| **УБИ2** | Н | Н | В | С | А |
| **УБИ3** | Н | Н | В | Н | А |
| **УБИ4** | Н | Н | В | С | А |
| **УБИ5** | Н | Н | В | С | А |
| **УБИ6** | Н | С | В | С | А |
| **УБИ7** | Н | Н | В | Н | А |
| **УБИ8** | Н | С | В | С | А |
| **УБИ9** | Н | В | В | В | А |
| **УБИ10** | Н | Н | В | Н | А |

**Меры защиты информации**

| **Ребро** | **Свойство** | **Угроза** | **Категория мер защиты** | **Подробно** |
| --- | --- | --- | --- | --- |
| Сервер → Бухгалтерия | Д | УБИ1 | Организационные | - Внедрение контроля доступа в помещения  - Введение видеонаблюдения  - Более тщательная проверка персонала  - Создание условий для соблюдения правил  - Пресечение действий нарушителей |
| Сервер → Бухгалтерия | К | УБИ2 | Технические,  Криптографические | - Код ревью  - Введение проверок  - Создание тестовой среды  - Шифрование данных, отправляемых на сервер |
| Доставка продовольствия → Сервер | К | УБИ3 | Организационные | - Проведение обучения персонала  - Более тщательная проверка персонала  - Создание условий для соблюдения правил |
| Сервер → Болельщик | К | УБИ4 | Технические,  Криптографические | - Проведение аудита веб-сайта и всей компании  - Шифрование данных, отправляемых на сервер |
| Сервер → Бухгалтерия | К | УБИ5 | Технические,  Криптографические | - Проведение аудита веб-сайта и всей компании  - Шифрование данных, отправляемых на сервер |
| Бухгалтерия → Сервер | К, Ц | УБИ6 | Технические,  Стеганографические | - Проведение аудита компании  - Введение проверок, в том числе нештатных  - Использование цифровых водяных знаков |
| Касса → Пассажиры | Ц | УБИ7 | Организационные,  Криптографические | - Создание условий для сохранения сотрудников  - Проведение обучения персонала  - Введение поощрений  - Увеличение заработных плат  - Шифрование данных, отправляемых на сервер |
| Сервер →  Банк | Д | УБИ8 | Организационные | - Внедрение контроля доступа в помещения  - Введение видеонаблюдения |
| Сервер → Пассажиры | Д | УБИ9 | Организационные | - Внедрение контроля доступа в помещения  - Введение видеонаблюдения |
| Касса →  Сервер | К, Ц | УБИ10 | Организационные,  Криптографические | - Создание условий для сохранения сотрудников  - Проведение обучения персонала  - Введение поощрений  - Шифрование данных, отправляемых на сервер |

**Итоговый список всех мер**

Организационные меры:

* Внедрение контроля доступа в помещения
* Введение видеонаблюдения
* Более тщательная проверка персонала
* Создание условий для соблюдения правил
* Пресечение действий нарушителей
* Создание условий для сохранения сотрудников
* Проведение обучения персонала
* Введение поощрений

Криптографические меры:

* Шифрование данных, отправляемых на сервер

Технические меры:

* Код ревью
* Создание тестовой среды
* Проведение аудита компании
* Введение проверок, в том числе нештатных
* Проведение аудита веб-сайта и всей компании

Стеганографические меры:

* Использование цифровых водяных знаков