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

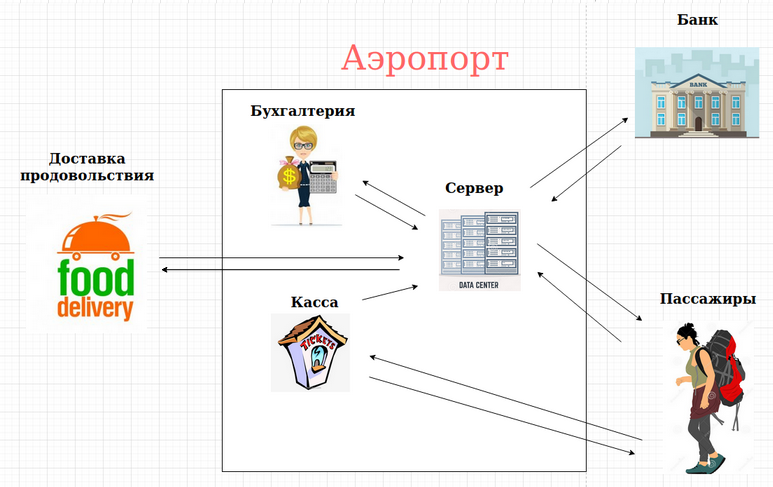
В качестве объекта информатизации был выбран аэропорт. Объект информатизации функционирует внутри одного здания.

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.

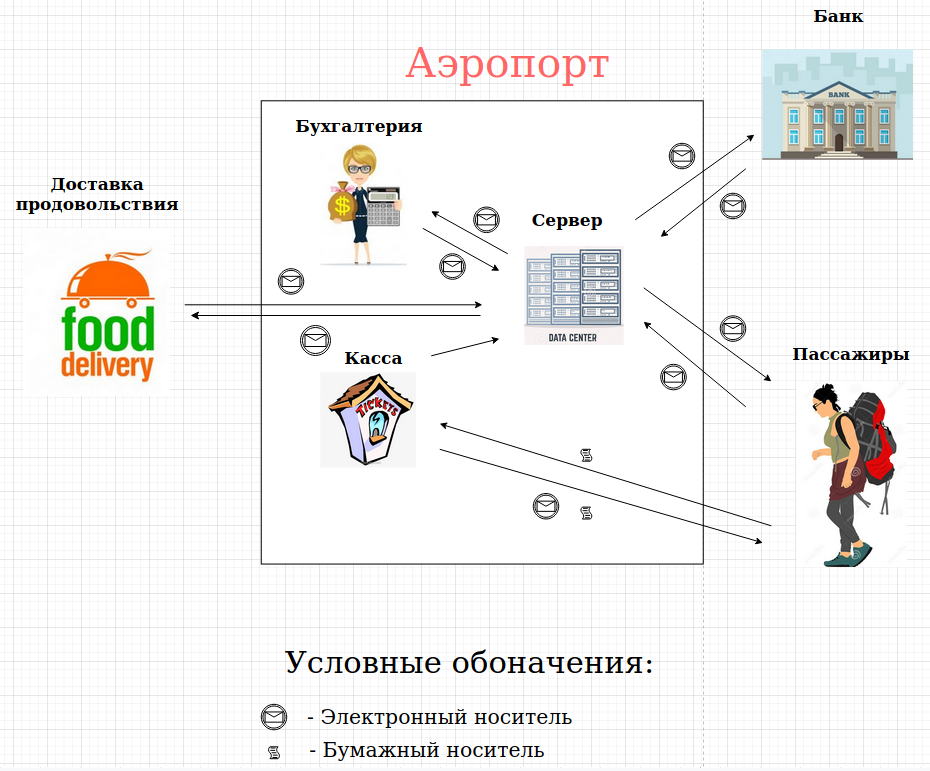
Денежные средства, поступающие от пассажиров учитываются в бухгалтерии, а затем отправляются в банк, с которым аэропорт взаимодействует через сервер. От сервера бане получает всю необходимую информацию, а затем загружает туда данные о транзакциях.

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

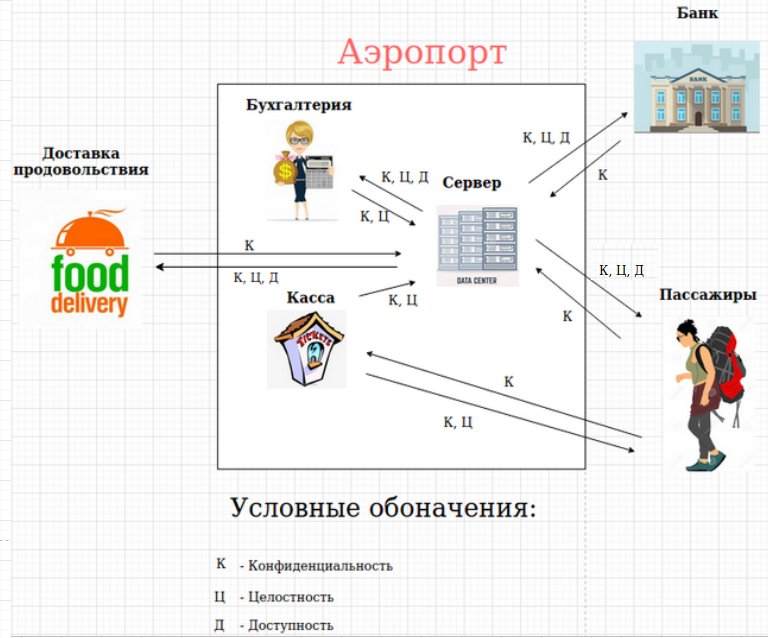


**Способы передачи данных**

**

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**



**Передаваемая информация**

| Номер | Откуда → Куда  (Свойства информации, которые необходимо обеспечить) | Что передаётся |
| --- | --- | --- |
| 1 | Пассажиры → Касса  (К) | Для покупки билета на кассе пассажир предоставляет свои паспортные данные и персональные данные(телефон для связи и почту для отправки билета) |
| 2 | Касса → Пассажиры  (К, Ц) | Кассир смотрит в БД свободны места на самолёте и печатает билет, выбранный пассажиром. Так же информация о билете отправляется на почту пассажира |
| 3 | Пассажиры → Сервер  (К) | На сервере крутится сайт для покупки авиабилетов. Пассажир загружает туда свои паспортные и персональные данные |
| 4 | Сервер → Пассажиры  (К, Ц, Д) | На сервере круглосуточно работает сайт. Сервер отправляет на почту пассажира его авиабилет. |
| 5 | Касса → Сервер  (К, Ц) | Кассир сканирует паспортные данные пассажира и вместе с выбранным им билетом отправляет на сервер. |
| 6 | Доставка продовольствия →Сервер  (К) | Внешние поставщики передают на сервер коммерческие предложения о заключении контрактов на поставку провизии. |
| 7 | Сервер → Доставка продовольствия  (К, Ц, Д) | На сервере крутится сайт с требованиями к необходимой продукции. В случае согласования контракта, все необходимые договора с сервера отправляются поставщику. |
| 8 | Бухгалтерия →Сервер  (К, Ц) | Бухгалтерию загружают на сервер финансовые отчёты, а также требования к продукции, необходимой аэропорту |
| 9 | Сервер → Бухгалтерия  (К, Ц, Д) | При необходимости бухгалтерии сервер выгружает всю необходимую информацию |
| 10 | Банк →Сервер  (К) | Передаются результаты транзакции |
| 11 | Сервер →Банк  (К, Ц, Д) | Отчёты по всем транзакциям передаются в банк с сервера |

**Угрозы безопасности информации**

**УБИ1 = [** Террорист, работающий в доставке продовольствия; отсутствия контроля на входе аэропорта; подрыв аэропорта; аэропорт; отказ в работе аэропорта **]**

(Д: Сервер → Пассажиры)

(Д: Сервер → Бухгалтерия)

(Д: Сервер → Доставщики продовольствия)

(Д: Сервер → Банк)

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

(К: Сервер → Банк)

(К: Сервер → Доставщики продовольствия)

**УБИ3** = [уволенный сотрудник аэропорта, устроившийся работать в доставку еды; низкая квалификация сотрудников аэропорта при составлении и проверки договоров; неправильное составление договора и отсутствие наказания за разглашение данных; договоры; нарушение конфиденциальности договоров]

(К: Доставка продовольствия→ Сервер)

**УБИ4 =** [хакер-любитель, ищущий уязвимости в интернете; наличие веб- уязвимостей на сайте; SQL-инъекция; база данных на сервере; доступ до данных на сервере]

(К: Сервер→ Пассажиры)

**УБИ5 =** [хакер- уборщик, убирающий в сервере; отсутствие видеонаблюдения и контроля за обслуживающим персоналом; намеренное изменение конфигурации сервера; сервер; доступ внутренних сотрудников до данных бухгалтерии]

(К: Сервер→ Бухгалтерия)

(К: Бухгалтерия → Сервер)

**УБИ6 =** [бухгалтер «под прикрытием», работающий на другую компанию; отсутствия контроля данных, отправляемых на сервер; модификация финансовых отчётов; рейтинг и репутация аэропорта; проблемы с налоговой]

(Ц: Бухгалтерия → Сервер)

**УБИ7 =** [кассир; плохое отношение к сотрудникам; доступ к приобретаемым билетам; билеты пассажиров; модификация и разглашение данных о пассажирах и их билетах]

(Ц: Касса→ Пассажиры)

(К: Пассажиры →Касса)

(К: Касса →Пассажиры)

**УБИ8 =** [шпион; передача данных от кассы к серверу по открытому каналу связи; прослушивание канала и перехват/модификация передаваемой информации; данные пассажиров; потеря данных пассажиров]

(К, Ц: Касса→ Сервер)

**УБИ9 =** [мастер по вызову, обслуживающий сервер; отсутствие наказания за умышленные действия, направленные во вред компании; модификация сервера, с целью обеспечения возможности проведение атаки Man In The Middle; данные на сервере; контроль передаваемой информации]

(К: Сервер→ Бухгалтерия)

(К: Банк → Сервер)

**УБИ10 =** [верстальщик сайтов; заключение договора с непроверенными компании; неправильное конфигурирование полей ввода, в результате которого к пользовательскому вводу добавляется лишняя информация; пользовательские данные; изменение вводимых пользователями данных]

(Ц: Сервер→ Пассажиры)

(Ц: Сервер → Доставщики продовольствия)

**УБИ11 =** [программист; отсутствие ИТ- архитектора в компании; неправильное хранение cookie, что позволяет пользователю проходить не свою аутентификацию; личные кабинеты пользователей; компрометация личных кабинетов пассажиров]

(К: Пассажиры→ Сервер)

**УБИ12 =** [студент, проходящий практику в качестве помощника системного администратора; беспорядок в серверной; нечаянное задевание аппаратуры, в результате которого, происходит отсоединение провода; серверная; часть данных не передаётся]

(Ц: Сервер→ Банк)

**Формальные модели нарушителей**

| Нарушитель | Тип | Вид | Потенциал | Цель | Возможные способы реализации угроз |
| --- | --- | --- | --- | --- | --- |
| Террорист  (УБИ1) | Внешний | Террористические, экстремистские группировки | Базовый повышенный | Организация террористического акта | Несанкционированной доступ и воздействие на объекты на общесистемном уровне |
| Сис. админ  (УБИ2) | Внутренний | Администраторы информационной системы и администраторы безопасности | Базовый повышенный | Реализация угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий | Несанкционированный физический доступ и воздействие на линии связи |
| Уволенный сотрудник аэропорта  (УБИ3) | Внешний | Бывшие работники | Базовый низкий | Реализация угроз безопасности информации из мести | Несанкционированный физический доступ и воздействие на линии связи |
| Хакер- любитель  (УБИ4) | Внешний | Внешние субъекты | Базовый низкий | Любопытство или желание самореализации | Воздействие на объекты на прикладном уровне |
| Хакер- уборщик  (УБИ5) | Внутренний | Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктура оператора | Базовый низкий | Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технических средства на этапе разработки | Несанкционированный физический доступ |
| Бухгалтер  (УБИ6) | Внутренний | Конкурирующие организации | Базовый повышенный | Получение конкурентных преимуществ | Несанкционированный физический доступ и воздействие на линии связи |
| Кассир  (УБИ7) | Внутренний | Пользователи информационной системы | Базовый низкий | Причинение имущественного ущерба путём мошенничества или иным преступным путём | Социальная инженерия |
| Шпион  (УБИ8) | Внешний | Внешние субъекты | Базовый низкий | Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды | Несанкционированный доступ и воздействие на объекты на сетевом уровне |
| Мастер по вызову  (УБИ9) | Внешний | Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ | Базовый низкий | Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды | Несанкционированный доступ и воздействие на объекты на аппаратном уровне |
| Верстальщик сайтов  (УБИ10) | Внешний | Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ | Базовый низкий | Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технических средства на этапе разработки | Несанкционированной доступ и воздействие на объекты на общесистемном уровне |
| Программист(УБИ11) | Внутренний | Разработчики, производители, поставщики программных, технических и программно-технических средств | Базовый повышенный | Реализация угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий | Несанкционированный доступ и воздействие на объекты на прикладном уровне (браузер) |
| Студент  (УБИ12) | Внешний | Пользователи информационной системы | Базовый низкий | Непреднамеренные, неосторожные или неквалифицированные действий | Несанкционированный физический доступ |

***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 | С | В | В | А |
| **УБИ2** | Н | С | В | Н | А |
| **УБИ3** | Н | Н | В | Н | А |
| **УБИ4** | Н | Н | В | Н | А |
| **УБИ5** | Н | Н | В | Н | А |
| **УБИ6** | Н | С | В | В | А |
| **УБИ7** | Н | Н | В | С | А |
| **УБИ8** | Н | Н | В | С | А |
| **УБИ9** | Н | Н | В | Н | А |
| **УБИ10** | Н | Н | В | С | А |
| **УБИ11** | Н | С | В | С | А |
| **УБИ12** | Н | Н | В | С | А |

**Меры защиты информации**

| **Ребро** | **Свойство** | **Угроза** | **Категория мер защиты** | **Подробно** |
| --- | --- | --- | --- | --- |
| Сервер →  Пассажиры, Бухгалтерия,  Доставка,  Банк | Д | УБИ1 | Организационные | -Внедрение контроля доступа в помещения  -Введение видеонаблюдения  -Более тщательная проверка персонала и людей  -Создание условий для соблюдения правил  - Введение проверок |
| Сервер → Банк | К | УБИ2 | Организационные,  Технические | - Код ревью  - Проверки сделанной работы  - Создание тестовой среды |
| Доставка продовольствия → Сервер | К | УБИ3 | Организационные | -Создание условий для соблюдения правил  - Проведение обучения персонала  - Создание условий для сохранения персонала  - Внедрение поощрений |
| Сервер → Пассажиры | К | УБИ4 | Технические,  Криптографические меры | -Проведение аудита веб-сайта и всей компании  - Шифрование передаваемых данных, а также данных, хранящихся на самом сервере  - Введение проверок |
| Сервер → Бухгалтерия  Бухгалтерия → Сервер | К | УБИ5 | Технические ,  Организационные | -Внедрение контроля доступа в помещения  -Введение видеонаблюдения  -Более тщательная проверка персонала и людей |
| Бухгалтерия → Сервер | Ц | УБИ6 | Организационные,  Технические | - Проверка персонала перед приёмом на работу  - Контроль за работой сотрудников  - Контроль за финансовыми потоками |
| Пассажиры →Касса  Касса →Пассажиры | К, Ц | УБИ7 | Организационные | - Создание условий для сохранения персонала  - Внедрение поощрений  - Контроль за состоянием сотрудников  - Создание условий для соблюдения правил |
| Касса → Сервер | К, Ц | УБИ8 | Криптографические | - Шифрование данных |
| Сервер → Бухгалтерия  Банк → Сервер | К | УБИ9 | Организационные,  Криптографические,  Стеганографические | - Шифрование данных  - Использование водяных знаков  - Контроль за работниками по найму  - Тщательный выбор работников по найму |
| Сервер →  Пассажиры, Доставка | Ц | УБИ10 | Организационные | - Создание законов(правил) заключения контрактов  - Проверка заказчиков и сделанной работы перед подписанием договора и оплатой |
| Пассажиры→ Сервер | К | УБИ11 | Организационные  Технические | - Код ревью  - Контроль всего процесса разработки в целом  -Проведение аудита веб-сайта и всей компании |
| Сервер → Банк | Ц | УБИ12 | Организационные | - Наведение порядка в серверной  - Организация удобных рабочих мест |

**Итоговый список всех мер**

Организационные меры:

Законодательные:

* Создание законов(правил) заключения контрактов

Морально — этические:

* Введение поощрений

Административные:

* Проверка заказчиков и сделанной работы перед подписанием договора и оплатой
* Более тщательная проверка персонала
* Создание условий для соблюдения правил
* Создание условий для сохранения сотрудников
* Проведение обучения персонала

Организационно - технические:

* Внедрение контроля доступа в помещения
* Введение видеонаблюдения

Криптографические меры:

* Шифрование данных, отправляемых на сервер

Технические меры:

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

Стеганографические меры:

* Использование цифровых водяных знаков