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

Содержание

[Введение 3](#__RefHeading___Toc1581_4020003460)

[Объект информатизации — Аэропорт 4](#__RefHeading___Toc1583_4020003460)

[Способы передачи данных 5](#__RefHeading___Toc1585_4020003460)

[Свойства информации, которые необходимо обеспечить 6](#__RefHeading___Toc1587_4020003460)

[Передаваемая информация 7](#__RefHeading___Toc1371_4020003460)

[Угрозы безопасности информации 8](#__RefHeading___Toc1589_4020003460)

[Формальные модели нарушителей 10](#__RefHeading___Toc1591_4020003460)

[Уровень проектной защищенности 12](#__RefHeading___Toc1593_4020003460)

[Степень реализации угроз 13](#__RefHeading___Toc1595_4020003460)

[Актуальность угроз 16](#__RefHeading___Toc1597_4020003460)

[Меры защиты информации 17](#__RefHeading___Toc1599_4020003460)

[Итоговый список всех мер 19](#__RefHeading___Toc1601_4020003460)

# Введение

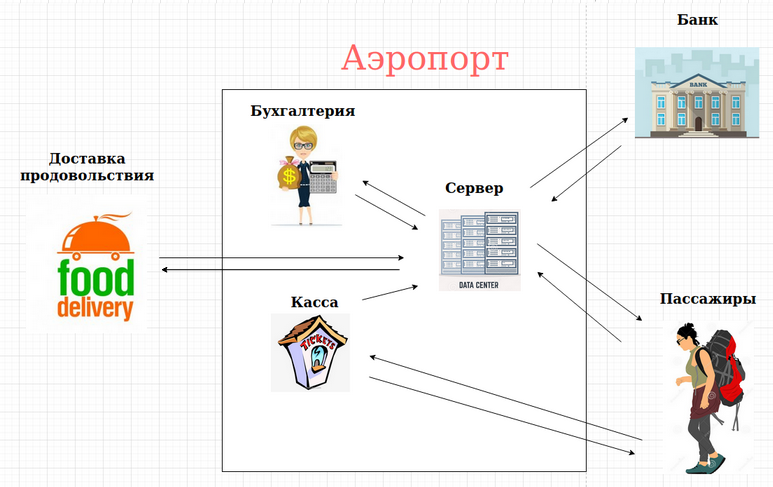
В качестве объекта информатизации был выбран аэропорт. Объект информатизации функционирует внутри одного здания.

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.

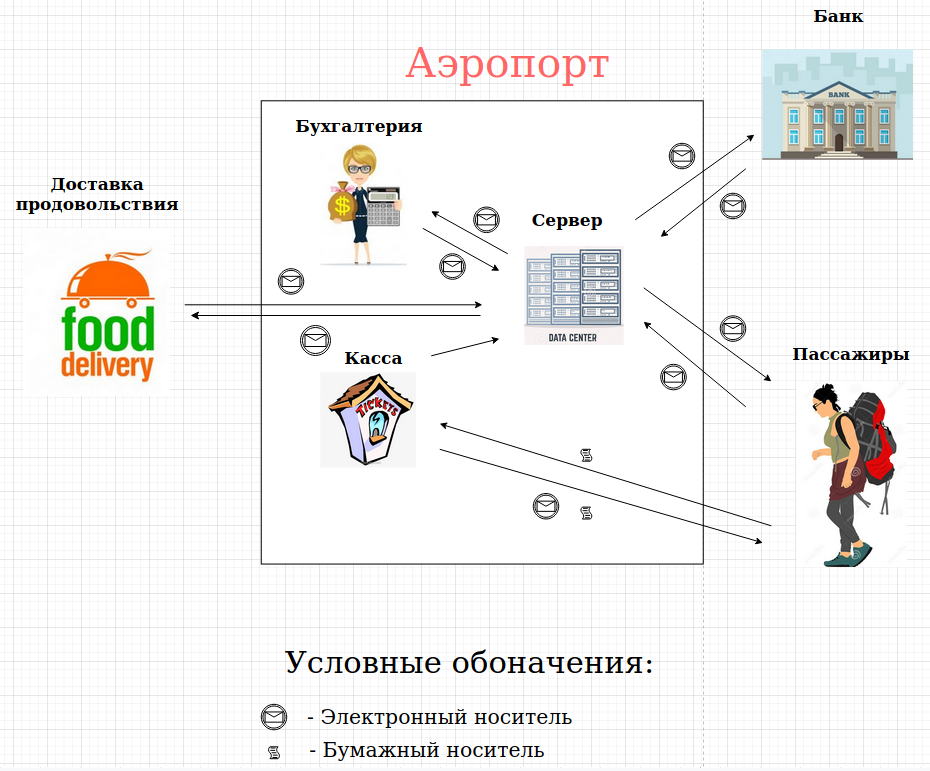
Денежные средства, поступающие от пассажиров учитываются в бухгалтерии, а затем отправляются в банк, с которым аэропорт взаимодействует через сервер. От сервера банк получает всю необходимую информацию, а затем загружает туда данные о транзакциях.

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

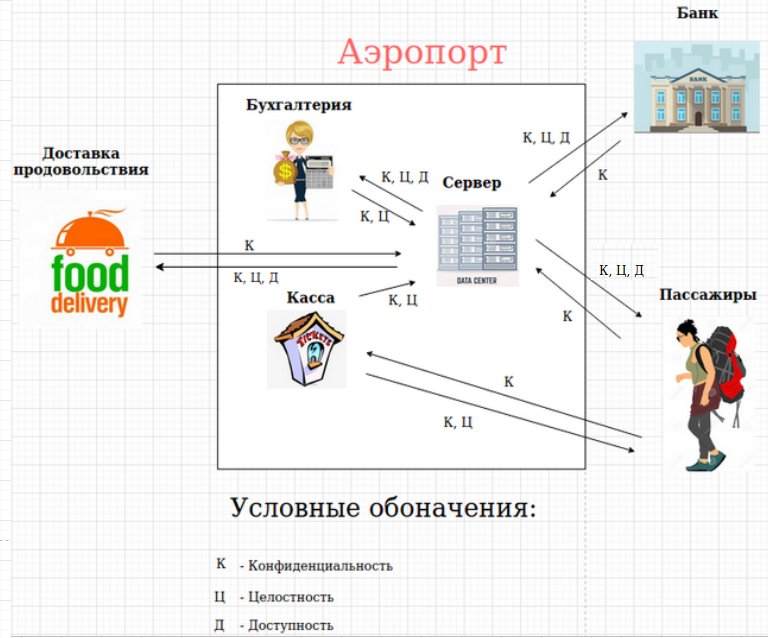


# Способы передачи данных

**

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

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

# Угрозы безопасности информации

**УБИ1 =** [террорист; 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 =** [администратор безопасности; низкая квалификация сотрудников; неправильное конфигурирование сервера; сервер; утечка данных на сервере]

(К: Сервер → Банк)

(К: Сервер → Доставщики продовольствия)

**УБИ3** = [уволенный сотрудник аэропорта; отсутствие проверки файлов перед скачиванием; намеренное заражение сервера троянской программой; сервер; доступ к данным на сервере]

(К: Доставка продовольствия→ Сервер)

**УБИ4 =** [хакер; наличие веб-уязвимостей на сайте; SQL-инъекция; база данных на сервере; доступ к данных на сервере]

(К: Сервер→ Пассажиры)

**УБИ5 =** [уборщик; отсутствие видеонаблюдения и контроля за обслуживающим персоналом; намеренное изменение конфигурации сервера; сервер; несанкционированный доступ внутренних сотрудников к данным бухгалтерии]

(К: Сервер→ Бухгалтерия)

(К: Бухгалтерия → Сервер)

**УБИ6 =** [подставной бухгалтер; отсутствия аудита данных, отправляемых на сервер; модификация финансовых отчётов; финансовые отчёты; закрытие аэропорта из-за финансового мошенничества]

(Ц: Бухгалтерия → Сервер)

**УБИ7 =** [кассир; плохое отношение к сотрудникам; намеренное разглашение и неправильное оформление билетов пассажиров; билеты пассажиров; нарушение функционирования аэропорта, падение количества клиентов аэропорта]

(Ц: Касса→ Пассажиры)

(К: Пассажиры →Касса)

(К: Касса →Пассажиры)

**УБИ8 =** [шпион; передача данных от кассы к серверу по открытому каналу связи; прослушивание канала; данные пассажиров; модификация и разглашение данных о пассажирах и их билетах]

(К, Ц: Касса→ Сервер)

**УБИ9 =** [поставщик ПО; отсутствие проверки покупаемого оборудования; внедрение нерегламентированных возможностей; сервер; доступ к серверу, контроль над передачи информации]

(К: Сервер→ Бухгалтерия)

(К: Банк → Сервер)

(К: Пассажиры→ Сервер)

**УБИ10 =** [верстальщик-конкурент; отсутствие проверки сторонних компаний перед заключением договора; неправильное конфигурирование полей ввода; пользовательские данные; изменение вводимых пользователями данных]

(Ц: Сервер→ Пассажиры)

(Ц: Сервер → Доставщики продовольствия)

**УБИ11 =** [студент, проходящий практику; беспорядок в серверной; случайное повреждение проводов в серверной; сервер; выключение сервера, невозможность полноценной работы компании]

(Ц: Сервер→ Банк)

# Формальные модели нарушителей

| Нарушитель | Тип | Вид | Потенциал | Цель | Возможные способы реализации угроз |
| --- | --- | --- | --- | --- | --- |
| Террорист | Внешний | Террористические, экстремистские группировки | Базовый повышенный | Совершение террористических актов | Несанкционированный физический доступ и воздействие на линии связи |
| Админ. безопасности | Внутренний | Администраторы информационной системы и администраторы безопасности | Базовый повышенный | Непреднамеренные, неосторожные или неквалифицированные действия | Воздействие на объекты на сетевом уровне |
| Уволенный сотрудник аэропорта | Внешний | Бывшие работники | Базовый низкий | Месть за ранее совершенные действия | Воздействие на объекты на прикладном уровне |
| Хакер | Внешний | Внешние субъекты | Базовый низкий | Любопытство или желание самореализации | Воздействие на объекты на прикладном уровне |
| Уборщик | Внутренний | Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктура оператора | Базовый низкий | Причинение имущественного ущерба путём обмана или злоупотребления доверием | Несанкционированный физический доступ и воздействие на линии связи |
| Подставной  бухгалтер | Внутренний | Пользователи информационной системы | Базовый низкий | Причинение  имущественного ущерба путём мошенничества или иным преступным путём | Воздействие на объекты на прикладном уровне |
| Кассир | Внутренний | Пользователи информационной системы | Базовый низкий | Любопытство или желание самореализации | Воздействие на объекты на прикладном уровне |
| Шпион | Внешний | Внешние субъекты | Базовый низкий | Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды | Воздействие на линии(каналы) связи |
| Поставщик ПО | Внешний | Разработчики, производители, поставщики программных, технических и программно-технических средств | Базовый повышенный | Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технических средства на этапе разработки | Несанкционированный доступ и воздействие на объекты на аппаратном уровне |
| Верстальщик сайтов | Внешний | Конкурирующие организации | Базовый повышенный | Получение конкурентных преимуществ | Несанкционированной доступ и воздействие на объекты на общесистемном уровне |
| Студент | Внутренний | Пользователи информационной системы | Базовый низкий | Непреднамеренные, неосторожные или неквалифицированные действий | Несанкционированный физический доступ и воздействие на линии связи |

# 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**

# Степень реализации угроз

| УБИ | Нарушаемое свойство информации | Степень ущерба | Пояснение |
| --- | --- | --- | --- |
| 1 | Доступность | В | *Возможные негативные последствия:*   * Создание предпосылок для нанесения вреда здоровью граждан(Взрыв аэропорта) * Возможность нарушения функционирования объектов обеспечения жизнедеятельности граждан(Закрытие аэропорта) * Неспособность выполнения международных (двусторонних) договорных обязательств * Необходимость дополнительных (незапланированных) затрат на восстановление деятельности * Потеря клиентов, поставщиков |
| 2 | Конфиденциальность | Н | *Возможные негативные последствия:*   * Недополучение ожидаемой (прогнозируемой) прибыли * Потеря клиентов, поставщиков |
| 3 | Конфиденциальность | В | *Возможные негативные последствия:*   * Потеря клиентов * Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. * Появление негативных публикаций в общедоступных источниках * Увеличение количества жалоб в органы государственной власти или органы местного самоуправления * Утрата доверия * Неспособность выполнения договорных обязательств |
| 4 | Конфиденциальность | В | *Возможные негативные последствия:*   * Потеря клиентов * Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. * Появление негативных публикаций в общедоступных источниках * Увеличение количества жалоб в органы государственной власти или органы местного самоуправления * Утрата доверия |
| 5 | Конфиденциальность | С | *Возможные негативные последствия:*   * Потеря клиентов, поставщиков * Появление негативных публикаций в общедоступных ис-точниках * Нарушение деловой репутации * Утрата доверия |
| 6 | Целостность | В | *Возможные негативные последствия:*   * Потеря (кража) финансовых средств * Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций * Невозможность заключения договоров, соглашений * Возможность нарушения функционирования объектов обеспечения жизнедеятельности граждан * Увольнения * Невозможность заключения международных (двусторонних) договоров, соглашений * Снижение престижа * Нарушение деловой репутации |
| 7 | Конфиденциальность,  Целостность | Н | *Возможные негативные последствия:*   * Потеря клиентов, поставщиков * Снижение престижа * Утрата доверия |
| 8 | Конфиденциальность,  Целостность | Н | *Возможные негативные последствия:*   * Недополучение ожидаемой (прогнозируемой) прибыли * Потеря клиентов, поставщиков * Утрата доверия * Нарушение деловой репутации |
| 9 | Конфиденциальность | В | *Возможные негативные последствия:*   * Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств)(Заражённый сервер) * Нарушение деловой репутации * Потеря клиентов, поставщиков * Невозможность заключения договоров, соглашений |
| 10 | Целостность | С | *Возможные негативные последствия:*   * Возможность нарушения функционирования объектов обеспечения жизнедеятельности граждан(Сайт работает некорректно ) * Необходимость дополнительных (незапланированных) затрат на восстановление деятельности * Потеря клиентов, поставщиков * Появление негативных публикаций в общедоступных ис-точниках * Потеря конкурентного преимущества |
| 11 | Целостность | В | *Возможные негативные последствия:*   * Возможность нарушения функционирования объектов обеспечения жизнедеятельности граждан(Данные не передаются, невозможность взаимодействия) * Недополучение ожидаемой (прогнозируемой) прибыли * Необходимость дополнительных (незапланированных) затрат на восстановление деятельности * Потеря клиентов, поставщиков * Невозможность заключения международных (двусторонних) договоров, соглашений |

# Актуальность угроз

| УБИ | **Уровень проектной защищенности** | **Потенциал нарушителя** | **Возможность реализации угрозы** | **Степень ущерба** | **Актуальность угрозы** |
| --- | --- | --- | --- | --- | --- |
| **1** | Н | С | В | В | А |
| **2** | Н | С | В | Н | А |
| **3** | Н | Н | В | В | А |
| **4** | Н | Н | В | В | А |
| **5** | Н | Н | В | С | А |
| **6** | Н | Н | В | В | А |
| **7** | Н | Н | В | Н | А |
| **8** | Н | Н | В | Н | А |
| **9** | Н | С | В | В | А |
| **10** | Н | С | В | С | А |
| **11** | Н | Н | В | В | А |

# Меры защиты информации

| **Ребро** | **Свойство** | **Угроза** | **Категория мер защиты** | **Подробно** |
| --- | --- | --- | --- | --- |
| Сервер →  Пассажиры, Бухгалтерия,  Доставка,  Банк | Д | УБИ1 | Организационные | *Административные:*   * Организация пропускного режима * Проведение регулярного аудита   *Орг-техн:*   * Установка видеокамер * Установка металлодетекторов * Установка ленты интроскоп |
| Сервер → Банк | К | УБИ2 | Организационные | *Административные:*   * Код ревью * Создание тестовой среды * Проверка сделанной работы * Проверка кандидатов при трудоустройстве на работу |
| Доставка продовольствия → Сервер | К | УБИ3 | Организационные | *Административные:*   * Обучение персонала * Проверка файлов перед скачиванием * Установка антивирусного ПО * Инструкции по использованию антивирусного ПО * Обновление должностной инструкции * Проведение инструктажа сотрудников |
| Сервер → Пассажиры | К | УБИ4 | Организационные  Криптографические | *Административные:*   * Проведение регулярного аудита   *Криптографические:*   * Шифрование данных * Шифрование канала связи |
| Сервер → Бухгалтерия  Бухгалтерия → Сервер | К | УБИ5 | Организационные | *Административные:*   * Организация пропускного режима * Проведение регулярного аудита * Разработка регламента уборки особо важных помещений, таких как серверная   *Орг-техн:*   * Установка видеокамер |
| Бухгалтерия → Сервер | Ц | УБИ6 | Организационные | *Административные:*   * Проверка персонала перед приёмом на работу * Контроль за работой сотрудников * Контроль за финансовыми потоками |
| Пассажиры →Касса  Касса →Пассажиры | К, Ц | УБИ7 | Организационные | *Административные:*   * Контроль за психологическим состоянием сотрудников |
| Касса → Сервер | К, Ц | УБИ8 | Криптографические  Стеганографические | *Криптографические:*   * Шифрование данных * Шифрование канала связи   *Стеганографические:*   * Использование цифровых водяных знаков |
| Сервер → Бухгалтерия  Банк → Сервер  Пассажиры→ Сервер | К | УБИ9 | Организационные | *Административные:*   * Проверка компаний перед заключением договора * Проверка оборудования перед покупкой |
| Сервер →  Пассажиры, Доставка | Ц | УБИ10 | Организационные | *Административные:*   * Проверка заказчиков и сделанной работы перед подписанием договора |
| Сервер → Банк | Ц | УБИ11 | Организационные | *Административные:*   * Наведение порядка в серверной * Организация удобных рабочих мест |

# **Итоговый список всех мер**

Организационные меры:

Административные:

* Организация пропускного режима
* Обучение персонала
* Проведение аудита компании
* Проверка персонала перед приёмом на работу
* Проверка оборудования перед покупкой
* Контроль за работой сотрудников
* Контроль за финансовыми потоками
* Наведение порядка в серверной
* Организация удобных рабочих мест
* Проверка заказчиков и сделанной работы перед подписанием договора
* Инструкции по использованию ПО
* Обновление должностных инструкций
* Проведение инструктажа сотрудников и ознакомление с должностной инструкцией

Программно-технические:

* Создание резервной копии данных
* Установка антивирусного ПО

Организационно - технические:

* Установка видеокамер
* Установка металлодетекторов
* Установка лент Интроскоп

Криптографические меры:

* Шифрование канала связи
* Шифрование передаваемых данных

Стеганографические меры:

* Использование цифровых водяных знаков