Правительство Российской Федерации

Федеральное государственное автономное образовательное

учреждение высшего образования   
"Национальный исследовательский университет   
"Высшая школа экономики"

Московский институт электроники и математики им. А. Н. Тихонова

Департамент прикладной математики

ОТЧЕТ

по курсовой работе по дисциплине

«Основы информационной безопасности»

Выполнил студент гр. СКБ171

Астраханцев Роман Геннадьевич

Тема работы: **«Определение комплекса мер обеспечения защиты объекта информатизации от актуальных угроз безопасности информации»**

Москва, 2020 г.

Оглавление

[Аэропорт им. Егора Летова с источниками информации 3](#_Toc40900752)

[Уточнение потоков информации 4](#_Toc40900753)

[Способы передачи информации 5](#_Toc40900754)

[Свойства информации, которые необходимо обеспечить 6](#_Toc40900755)

[Угрозы безопасности информации 7](#_Toc40900756)

[Модели нарушителей 9](#_Toc40900757)

[Уровень проектной защищенности 12](#_Toc40900758)

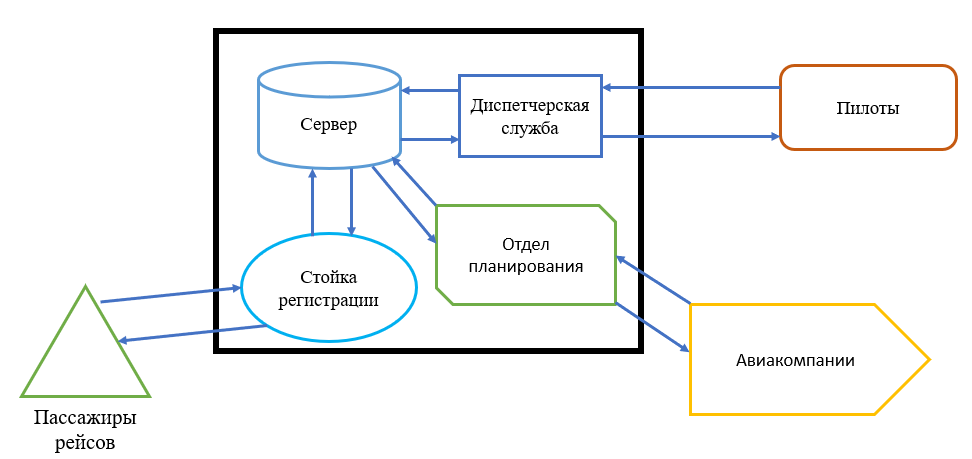
[Степень ущерба 13](#_Toc40900759)

[Актуальность угроз 14](#_Toc40900760)

[Меры защиты информации 15](#_Toc40900761)

[Итоговый список мер защиты информации 17](#_Toc40900762)

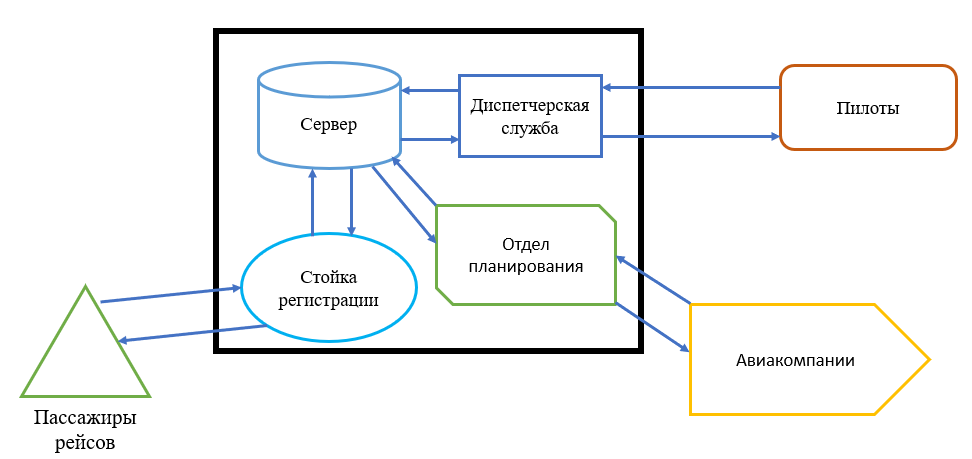
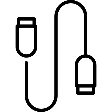
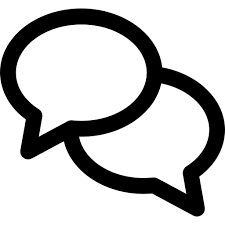
# **Аэропорт им. Егора Летова с источниками информации**



# **Уточнение потоков информации**

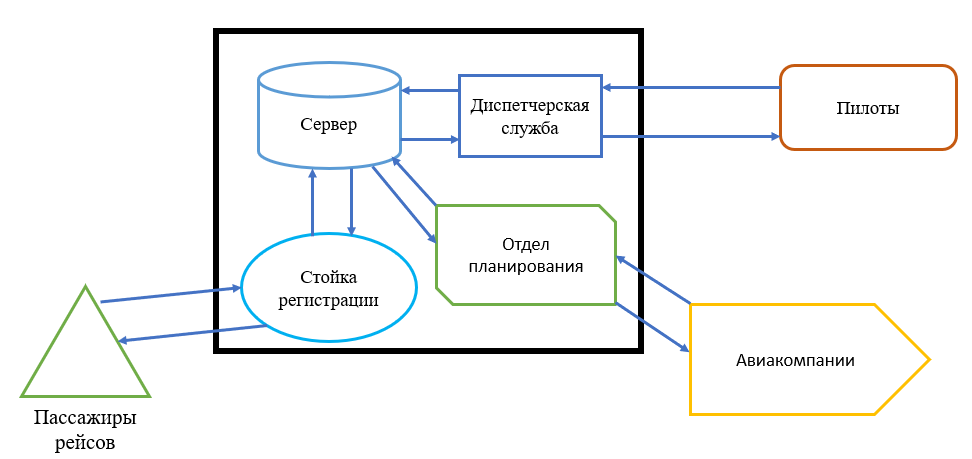
|  |  |
| --- | --- |
| **Поток** | **Дополнительная информация** |
| Пилот ⇒ Диспетчерская служба | Номер борта, полоса на которую заходишь и намерения (на стоянку, переждать, на заправку и т.д.) |
| Диспетчерская служба ⇒ Пилот | Вектор направления движения самолёта, разрешение на посадку |
| Сервер ⇒ Диспетчерская служба | Информация о наличии топлива, наличии свободной полосы, наличии парковочного места |
| Диспетчерская служба ⇒ Сервер | Запрашиваются на данные о наличии топлива, наличии свободной полосы, наличии парковочного места. Предаются регистрационные данные прилетевшего судна борта, факт прилёта/вылета. |
| Авиакомпания ⇒ Отдел планирования | Список рейсов на прилёт/отлёт, количество требуемых стояночных мест, количество требуемого топлива на даты соответствующих рейсов |
| Отдел планирования ⇒ Авиакомпания | Подтверждение получения информации, согласование возможности принятия рейсов на итоговую дату. |
| Отдел планирования ⇒ Сервер | Согласованные данные, полученные от авиакомпаний, затраты на покупку топлива. |
| Сервер ⇒ Отдел планирования | Количество топлива и посадочных мест для предоставления прилетающим бортам |
| Пассажиры рейсов ⇒ Стойка регистрации | Данные о брони, паспортные данные, информация о багаже |
| Стойка регистрации ⇒ Пассажиры рейсов | Посадочный талон |
| Стойка регистрации ⇒ Сервер | Запрос на наличие брони. Факт прибытия пассажира, информацию о багаже этого пассажира. |
| Сервер ⇒ Стойка регистрации | Талон на посадку для конкретного пассажира |

# **Способы передачи информации**



|  |  |  |  |
| --- | --- | --- | --- |
| Возникновение и распространение Радиоволн. | Кабель | Бесплатно значок | Листы бумаги значок векторное изображение | Векторы общественного ... | диалог, воздушный шар бесплатно значок из Outicons |
| **Радиоэфир** | **Электронный файл** | **Бумажный носитель** | **Посредством диалога** |

# **Свойства информации, которые необходимо обеспечить**



**К**

**К**

**Ц, Д, К**

**Ц, К**

**Ц, Д**

**Ц**

**Ц, К**

**Ц, Д**

**Ц**

**К**

**Ц**Ф

**Ц – Целостность, К – Конфиденциальность, Д - Доступность**

# **Угрозы безопасности информации**

УБИ1 = [террорист; открытость радиоэфира; включение устройства, нарушающего радиоэфир; радиоэфир; отсутствие возможности передачи информации по радиоэфиру (отсутствие связи между диспетчером и пилотом)];

(Свойство целостности: Диспетчерская служба ⇒ Пилот)

УБИ2 = [хакерская группировка; отсутствие приватной сети для работы сервера; внедрение вредоносного ПО; сервер аэропорта; кража данных с сервера];

(Свойство конфиденциальности: Отдел планирования ⇒ Сервер, Стойка рестрикции ⇒ Сервер, Сервер ⇒ Стойка регистрации)

УБИ3 = [уборщица; отсутствие регламента действий; затопление сервера; ведро с водой, комната с сервером; вывод сервера из строя];

(Свойство доступности: Сервер ⇒ Стойка отдел планирования, Сервер ⇒ Диспетчерская служба, Сервер ⇒ Стойка регистрации)

УБИ4 = [бывший администратор ИС; отсутствие регламента по смене пароля на сервере; проникновение на сервер и внедрение паразитических вирусов; сервер; изменение персональных данных и служебной информации];

(Свойство целостности: Сервер ⇒ Стойка отдел планирования, Сервер ⇒ Диспетчерская служба, Сервер ⇒ Стойка регистрации, Стойка отдел планирования ⇒ Сервер, Диспетчерская служба ⇒ Сервер, Стойка регистрации ⇒ Сервер)

УБИ5 = [сотрудник на стойке регистрации; отсутствие проверки сотрудника; найм злоумышленника на работу; стойка регистрации; кража персональных данных пассажиров];

(Свойство конфиденциальности: Стойка регистрации ⇒ Пассажиры рейсов, Пассажиры рейсов ⇒ Стойка регистрации)

УБИ6 = [авиакомпания-злоумышленник; отсутствие антивирусной программы; email-рассылка с вредоносными программами; ПК отдела планирования; кража данных других авиакомпаний о запланированных рейсах];

(Свойство конфиденциальности: Авиакомпании ⇒ Отдел планирования)

УБИ7 = [авиакомпания-злоумышленник; отсутствие проверки сотрудника; найм подставного сотрудника на работу; отдел планирования; Перехват и редактирование документов сообщения между авиакомпаниями и отделом планирования];

(Свойство целостности: Отдел планирования ⇒ Авиакомпании)

УБИ8 = [разработчик ПО; отсутствие системы тестирования ПО; ошибка в коде программы повлекшая некорректный ответ за запрос; диспетчер; нарушение корректной работы авиасообщения аэропорта (с потенциальным столкновением двух самолётов)]

(Свойство целостности: Сервер ⇒ Диспетчерская служба)

УБИ9 = [электрик; отсутствие дополнительного источника питания; ошибка работника; внутренняя система электропитания аэропорта; отключение электричества]

(Свойство доступности: Сервер ⇒ Стойка отдел планирования, Сервер ⇒ Диспетчерская служба, Сервер ⇒ Стойка регистрации)

(Свойство целостности: Сервер ⇒ Стойка отдел планирования, Сервер ⇒ Диспетчерская служба, Сервер ⇒ Стойка регистрации, Стойка отдел планирования ⇒ Сервер, Диспетчерская служба ⇒ Сервер, Стойка регистрации ⇒ Сервер)

(Свойство целостности: Диспетчерская служба ⇒ Пилот)

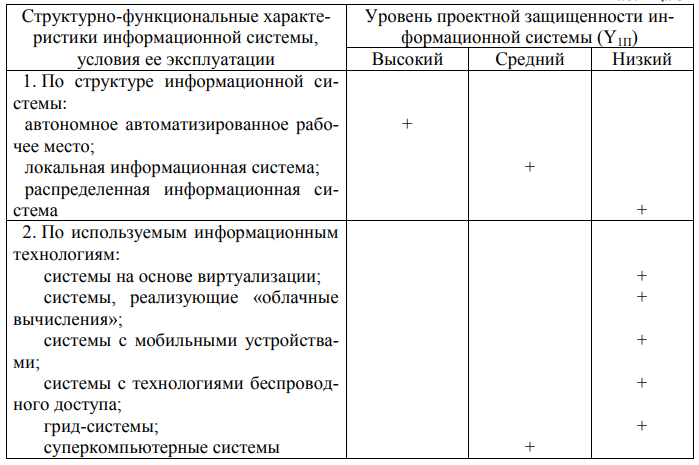
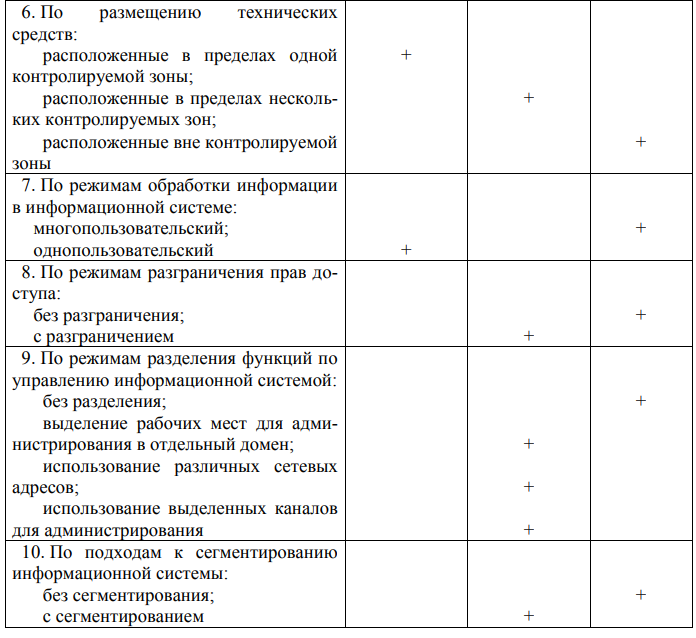
УБИ10 = [подставной курьер; отсутствие проверки документов курьера; передача посылки злоумышленнику; ответный документ от аэропорта к авиакомпании; изменение ответного сообщения];

(Свойство целостности: Отдел планирования ⇒ Авиакомпании)

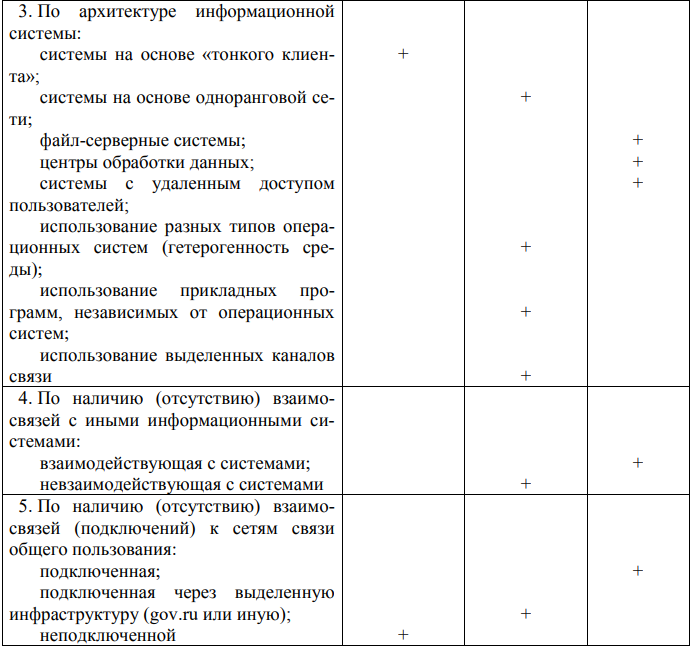
# **Модели нарушителей**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Нарушитель** | **Тип** | **Вид** | **Потенциал** | **Цели** | **Способы реализации** |
| Подставной курьер | Внутренний | Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора | Базовый | Получение конкурентных преимуществ | Воздействие на пользователей, администраторов безопасности, администраторов  информационной системы или обслуживающий персонал |
| Авиакомпания-злоумышленник | Внешний | Преступные группы | Базовый повышенный | Получение конкурентных преимуществ | Несанкционированный доступ и (или) воздействие на объекты на прикладном уровне |
| Подставной сотрудник на стройке регистрации | Внутренний | Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора | Базовый | Причинение имущественного ущерба путем мошенничества или иным преступным путем | Воздействие на пользователей, администраторов безопасности, администраторов  информационной системы или обслуживающий персонал |
| Подставной сотрудник в отделе планирования | Внутренний | Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора | Базовый | Получение конкурентных преимуществ | Воздействие на пользователей, администраторов безопасности, администраторов  информационной системы или обслуживающий персонал |
| Разработчик ПО | Внутренний | Разработчики, производители, поставщики программных, технических и программнотехнических средств | Базовый повышенный | Реализация угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий | Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне |
| Террорист, мешающий радиоэфиру | Внешний | Террористические, экстремистские группировки | Базовый повышенный | Организация террористического акта | Несанкционированный физический доступ и (или) воздействие на линии (каналы) связи,  технические средства, машинные носители информации |
| Администратор ИС | Внешний | Бывший сотрудник | Базовый | Реализация угроз безопасности информации из мести | Несанкционированной доступ и (или) воздействие на объекты на общесистемном уровне |
| Уборщица | Внутренний | Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора | Базовый | Реализация угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий | Несанкционированный физический доступ и (или) воздействие на линии (каналы) связи,  технические средства, машинные носители информации |
| Хакерская группировка | Внешний | Преступные группы | Базовый повышенный | Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды | Несанкционированный доступ и (или) воздействие на объекты на сетевом уровне |
| Электрик | Внутренний | Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора | Базовый | Реализация угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий | Несанкционированный физический доступ и (или) воздействие на линии (каналы) связи,  технические средства, машинные носители информации |

# **Уровень проектной защищенности**



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | *Высокий* | *Средний* | *Низкий* | | + | +  +  +  +  + | +  +  +  +  + |   *«+» в высоком и среднем уровне: 2 + 5 = 7*  *«+» всего 1 + 5 + 5 = 11*  *1/11 < 9/10 и 6/11 < 9/10 ⟶ уровень проектной защищённости низкий* |



# **Степень ущерба**

|  |  |  |  |
| --- | --- | --- | --- |
| УБИ | Свойство информации | Что произошло? | Степень ущерба |
| 1 | Ц | Сильные помехи в радиоэфире | В |
| 2 | К | Кража данных с сервера | Н |
| 3 | Д | Вывод сервера из строя | В |
| 4 | Ц | Изменение персональных данных и служебной информации | С |
| 5 | К | Кража персональных данных пассажиров | Н |
| 6 | К | Кража данных других авиакомпаний о запланированных рейсах | Н |
| 7 | Ц | Перехват и редактирование документов сообщения между авиакомпаниями и отделом планирования | Н |
| 8 | Ц | Нарушение корректной работы авиасообщения аэропорта (с потенциальным столкновением двух самолётов) | В |
| 9 | Ц, Д | Отключение электропитания | В |
| 10 | Ц | Изменение ответного сообщения от аэропорта к авиакомпании | Н |

# **Актуальность угроз**

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

# **Меры защиты информации**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Угроза | Ребро | Свойство | Категория мер защиты | Подробно |
| УБИ1 | Диспетчерская служба ⇒ Пилот | Ц | Меры технической ЗИ | Установка оборудования обнаружения и подавления радиопомех |
| Законодательные меры ЗИ | Направить обращение о запрете использования средств создания радиопомех в некотором радиусе вблизи аэропортов |
| УБИ2 | Отдел планирования ⇒ Сервер, Стойка рестрикции ⇒ Сервер, Сервер ⇒ Стойка регистрации | К | Меры технической ЗИ | Создание отдельной локальной сети или виртуальной сети для работы сервера |
| УБИ3 | Сервер ⇒ Стойка отдел планирования, Сервер ⇒ Диспетчерская служба, Сервер ⇒ Стойка регистрации | Д | Административные меры ЗИ | Организация регламента уборки помещений повышенной опасности, таких как серверные, генераторные комнаты и другие, а также создание условий для быстрого восстановления их работы. |
| УБИ4 | Сервер ⇒ Стойка отдел планирования, Сервер ⇒ Диспетчерская служба, Сервер ⇒ Стойка регистрации, Стойка отдел планирования ⇒ Сервер, Диспетчерская служба ⇒ Сервер, Стойка регистрации ⇒ Сервер | Ц | Организационно-технические меры ЗИ | Создание обязательного регламента по смене паролей на каждом компьютере/сервере при найме/увольнении сотрудника |
| УБИ5 | Стойка регистрации ⇒ Пассажиры рейсов, Пассажиры рейсов ⇒ Стойка регистрации | К | Административные меры ЗИ | Создание системы контроля за персоналом |
| Морально-этические меры ЗИ | Организация проверки персонала на предмет понимания последствий нарушения тех или иных законов/внутренних административных актов. |
| УБИ6 | Авиакомпании ⇒ Отдел планирования | К | Организационно-технические меры ЗИ | Установка антивирусной программы на всех компьютерах |
| УБИ7 | Отдел планирования ⇒ Авиакомпании | Ц | Административные меры ЗИ | Организация меры найма персонала с подробным рассмотрением истории работы, мотивации найма на работу, а также выявления возможности связи с преступными группировками нового сотрудника |
| УБИ8 | Сервер ⇒ Диспетчерская служба | Ц | Организационно-технические меры ЗИ | Развёртывание тестовой среды и регулярного тестирования на этапе разработки нового ПО |
| УБИ9 | Сервер ⇒ Стойка отдел планирования, Сервер ⇒ Диспетчерская служба, Сервер ⇒ Стойка регистрации  Стойка отдел планирования ⇒ Сервер, Диспетчерская служба ⇒ Сервер, Стойка регистрации ⇒ Сервер  Диспетчерская служба ⇒ Пилот | Д, Ц | Организационно-технические меры ЗИ | Организация работы бесперебойного питания |
| Меры технической ЗИ | Установка запасного источника питания аэропорта |
| УБИ10 | Отдел планирования ⇒ Авиакомпании | Ц | Административные меры ЗИ | Создание собственного отдела доставки письменных сообщений |

# **Итоговый список мер защиты информации**

* *Административные меры ЗИ:*
  + Организация регламента уборки помещений повышенной опасности, таких как серверные, генераторные комнаты и другие, а также создание условий для быстрого восстановления их работы
  + Создание системы контроля за персоналом
  + Организация меры найма персонала с подробным рассмотрением истории работы, мотивации найма на работу, а также выявления возможности связи с преступными группировками нового сотрудника
  + Создание собственного отдела доставки письменных сообщений
* *Организационно-технические меры ЗИ:*
  + Создание обязательного регламента по смене паролей на каждом компьютере/сервере при найме/увольнении сотрудника
  + Установка антивирусной программы на всех компьютерах
  + Развёртывание тестовой среды и регулярного тестирования на этапе разработки нового ПО
  + Организация работы бесперебойного питания
* *Законодательные меры ЗИ:*
  + Направить обращение о запрете использования средств создания радиопомех в некотором радиусе вблизи аэропортов
* *Морально-этические меры ЗИ:*
  + Организация проверки персонала на предмет понимания последствий нарушения тех или иных законов/внутренних административных актов.
* *Меры технической ЗИ*
  + Установка оборудования обнаружения и подавления радиопомех
  + Создание отдельной локальной сети или виртуальной сети для работы сервера
  + Установка запасного источника питания аэропорта