

Введение.....	2
1. Описательная модель системы радиочастотной идентификации как механизма защиты телекоммуникационной сети авиапредприятия от реализации сетевых атак	6
1.1 Телекоммуникационная сеть аэропорта как объект реализации сетевых атак.....	6
1.2 Системы радиочастотной идентификации как средство автоматизации обработки информации.....	11
1.3 Применение систем радиочастотной идентификации в телекоммуникационных сетях аэропорта.....	16
1.4 Классификация угроз информационной безопасности и атак в телекоммуникационной сети аэропорта, защищенной при помощи систем радиочастотной идентификации.....	20
1.5 Требования информационной безопасности, предъявляемые к телекоммуникационной сети аэропорта, защищенной при помощи систем радиочастотной идентификации.....	26
2 Оценка защищенности телекоммуникационной сети аэропорта с учетом внедрения системы радиочастотной идентификации	30
2.1 Постановка задачи исследования.....	30
2.2 Действия злоумышленника и последствия реализации атаки «IP - спуфинг» на телекоммуникационную сеть аэропорта, защищенную посредством внедрения системы радиочастотной идентификации	33
2.3 Разработка математической модели реализации удаленной атаки «IP-спуфинг» на телекоммуникационную сеть аэропорта, защищенную посредством внедрения системы радиочастотной идентификации	36
2.4 Оценка эффективности защиты информации телекоммуникационной сети аэропорта посредством системы радиочастотной идентификации	43
Заключение	
Список использованной литературы....	Ошибка! Закладка не определена.

Для современного этапа развития общества характерен непрерывный процесс информатизации и совершенствования информационных технологий. С внедрением информационных технологий во все сферы жизнедеятельности человека проблемы информационной безопасности (ИБ) с каждым годом становятся все более сложными и многогранными. Проблема обеспечения информационной безопасности (ИБ) постоянно усугубляется процессами проникновения технических средств обработки и передачи данных во все сферы деятельности общества. На любом, даже самом маленьком предприятии, присутствуют средства вычислительной техники, обрабатывающие информацию. Область применения телекоммуникационных систем также не является исключением и постоянно расширяется, при этом, на такие системы возлагается существенная ответственность не только за повышение качества и эффективности работы, но и за безопасность информации.

Не являются исключением и телекоммуникационные системы авиапредприятий, основной задачей которых является обеспечение высокого уровня безопасности полетов и эффективности обслуживания пассажиров.

Уязвимость телекоммуникационной сети авиапредприятий существенно превышает уязвимость отдельно взятых узлов. Это связано, прежде всего с масштабностью и неоднородностью самих автоматизированных информационных систем. При этом число угроз информационной безопасности и способов их реализации постоянно растет. Основными причинами являются здесь рост сложности программно-аппаратных средств и недостатки современных информационных технологий. С учетом того, что любая телекоммуникационная сеть авиапредприятия в той или иной части имеет доступ к сети Интернет, наиболее актуальными угрозами безопасности на сегодняшний день являются угрозы реализации удаленных атак и распространения вредоносной

информации через сеть.

Без использования систем и средств обеспечения ИБ в телекоммуникационной сети авиапредприятия возникает угроза хищения или уничтожения персональных данных, критически важной корпоративной или конфиденциальной информации. Таким образом, нарушение целостности, уничтожение или хищение данных телекоммуникационной сети авиапредприятия может привести к причинению ущерба различного масштаба. При этом любые нарушения и сбои в работе телекоммуникационной сети авиапредприятия могут грозить не только колоссальными финансовыми потерями, но и наносить ущерб жизни и здоровью людей. Это еще раз подтверждает, что исследования в области защиты информации на авиапредприятии являются важными не только для защиты информационных сервисов самой сети, но и для поддержания национальной безопасности.

В этой связи вытекает необходимость обеспечения достаточной степени защищенности телекоммуникационной сети авиапредприятия для его эффективного функционирования, а также снижения уровня риска от реализации внутренних и внешних угроз и, в конечном счете, повышения защищенности сети. Одним из механизмов повышения информационной безопасности является внедрение системы радиочастотной идентификации, которая заключается в идентификации объектов посредством радиосигналов. Такими системами считываются или записываются данные, хранящиеся в так называемых транспондерах, или RFID-метках. В нашей работе необходимо оценить влияние внедрения систем радиочастотной идентификации в телекоммуникационную сеть авиапредприятия.

В настоящее время активно ведется изучение защищенности телекоммуникационной сети авиапредприятия в контексте реализации удаленных сетевых атак. Непредсказуемость таких атак не позволяет создать детерминированное описание этих процессов и возникающих от их реализации ущербов. Поэтому, при создании защищенных

телекоммуникационных сетей авиапредприятий, вполне обоснованно моделирование ущерба от реализации удаленных сетевых атак как случайной величины.

Таким образом, исходя из актуальности и степени научной разработанности проблемы нарастания ущерба реализации удаленных сетевых атак можно сделать вывод о целесообразности проведения комплексных исследований в направлении построения математической модели телекоммуникационной сети авиапредприятия с учетом внедрения системы радиочастотной идентификации и изучения защищенности сети.

Объектом исследования является телекоммуникационная сеть авиапредприятия, защищенная посредством системы радиочастотной идентификации.

Предметом исследования является оценка эффективности защиты системы радиочастотной идентификации в условиях реализации удаленных сетевых атак.

Цели и задачи исследования.

Цель настоящей работы заключается в разработке математической модели телекоммуникационной сети авиапредприятия с учетом внедрения системы радиочастотной идентификации и изучения защищенности сети. Для достижения указанной цели предполагается решить следующие задачи:

1. Провести анализ основных видов удаленных сетевых атак, воздействующих на телекоммуникационную сеть авиапредприятия, защищенной посредством системы радиочастотной идентификации.

2. Построить описательную и математическую модель телекоммуникационной сети авиапредприятия, защищенной посредством системы радиочастотной идентификации, как среды реализации удаленных сетевых атак.

3. Провести анализ эффективности защиты телекоммуникационной сети авиапредприятия и эффективности работы системы радиочастотной идентификации при реализации удаленных сетевых атак.

4. Разработать рекомендации по использованию математической модели для обеспечения информационной безопасности телекоммуникационной сети авиапредприятия.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в дипломной работе, обеспечивается корректным использованием математических методов в приложении обозначенному предмету исследования.

В исследовании предполагается использовать методы теории вероятности, методы математической статистики и статистического анализа, методы теории графов, методы аналитического моделирования.

I