

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГРАЖДАНСКОЙ АВИАЦИИ**Федосеева Мария Сергеевна**

Студентка 2-го курса Московского политехнического университета

**Панов Николай Николаевич**

Капитан полиции, начальника отдела охраны комплексной безопасности Московского политехнического университета

Аннотация. В данной работе рассматривается обеспечение информационной безопасности корпоративных систем аэропорта. Проанализированы потенциальные угрозы безопасности информационной системы аэропорта. Выявлена и обоснована необходимость совместного использования программно-аппаратного и административного методов защиты информации. На основе проведенного исследования разработаны рекомендации по улучшению защиты информации, используемой в гражданской авиации.

Ключевые слова: безопасность, информация, аэропорт, защита, угрозы, уязвимости, риски.

Annotation. In this paper we consider the information security of corporate systems of the airport. The potential threats to the security of the airport information system are analyzed. The necessity of joint use of hardware-software and administrative methods of information security is revealed and substantiated. On the basis of the study recommendations for improving the protection of information used in civil aviation were developed.

Keywords: security, information, airport, protection, threats, vulnerabilities, risks.

Введение

В современной России насчитывается более 1200 аэропортов, которые обеспечивают граждан воздушными перевозками. Не менее 10 000 самолетов пролетают в небе ежедневно, огромное количество информации передается постоянно в аэропорте. Развитие Интернет-технологий способствовало увеличению серьезных угроз разглашения важных корпоративных ресурсов, государственных тайн, конфиденциальных данных. Злоумышленники постоянно ищут способы проникновения в доступ корпоративной системы, хранящей информацию о пассажирах, полетах, самолетах. Международная организация гражданской авиации (ИКАО) стала прилагать больше сил на решение проблем, связанных с защитой информации, используемой в объектах гражданской авиации.

Цель исследования

Изучить обеспечение информационной безопасности гражданской авиации.

Задачи исследования

- Проанализировать угрозы информационной системы аэропорта.
- Рассмотреть методы защиты информационной системы аэропорта.
- Разработать рекомендации по улучшению защиты информации, используемой в гражданской авиации.

Результаты исследования

Такая корпоративная сеть как аэропорт обрабатывает ценную информацию, однако является уязвимой из-за широкого использования глобальной сети Интернет, повышения количества передающихся данных и числа пользователей, имеющих непосредственный доступ к файлам системы, и хранения информации различного уровня конфиденциальности.

Последние исследования в британской аудиторско-консалтинговой компании Ernst&Young (рис. 1) показывают, что вирусы, противоправные действия работников и спам составляют пятерку основных рисков внутренней безопасности.

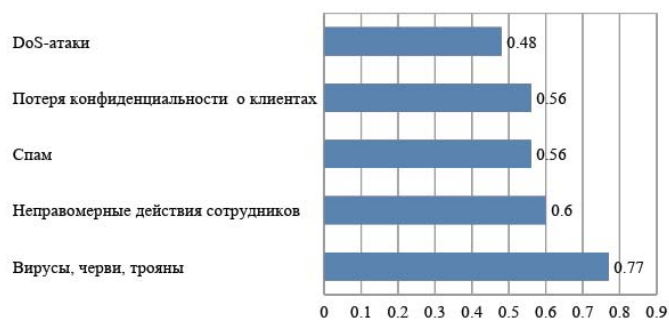


Рис. 1. Топ-5 угроз информационной безопасности

Самыми распространенными угрозами в информационной системе являются неправильные действия пользователей. Такие ошибки способны привести к остановке системы. Часто пользователь ненамеренно создает уязвимые точки, привлечь которые могут злоумышленники.

Не менее опасными угрозами являются кражи. Если не контролировать работу информационного канала связи, то такое положение способствует неправомерной деятельности [1].

В аэропорте чаще всего пользуются беспроводными сетями, сигнал которых перехватить несложно, применяя соответствующие средства.

Наиболее распространенные уязвимости и угрозы беспроводных сетей представлены в табл. 1.

Таблица 1

Наиболее распространенные уязвимости и угрозы беспроводных сетей

Угроза	Основная информация
Вещание радиомаяка	Используя широкоэвещательный радиомаяк, точка доступа раздает узлам сигналы, содержащие основную информацию, включая Service Set Identifier (SSID – идентификатор беспроводной сети) и сообщают о регистрации в данном секторе. Пользователи устройств могут присвоить SSID и стать участником сети
Обнаружение WLAN	Существуют утилиты, способные обнаружить беспроводные сети при помощи GPS (глобальной системы позиционирования) для идентификации SSID сети и определения типа шифрования
Подслушивание	Перед атакой правонарушители собирают данные о сети, используя их для получения доступа к сетевым ресурсам
Ложные точки доступа в сети	Пользователи передают персональные данные на неверную станцию

Отказ в обслуживании (DoS-атака)	Данная угроза предназначена создавать помехи устройствам, пытающимся получить доступ к сетевым ресурсам
Атаки типа «человек в середине»	Изменяя идентификацию сетевого ресурса, злоумышленник может прослушивать, получать и изменять данные пользователя
Анонимный доступ в Интернет	Используя открытую сеть, злоумышленник может действовать незаконно, оставаясь незамеченным.

Многопользовательская сеть обработки данных аэропорта имеет класс защищенности 1Г. Это означает, что в данной системе должна осуществляться идентификация субъектов, имеющих определенные права пользователей, по определенному паролю и быть обеспечена целостность программных средств.

Методами защиты информационной системы аэропорта являются программно-аппаратные и административные способы [2, 3].

Программно-аппаратные способы защиты информационной системы аэропорта представлены на рис. 2.



Рис. 2. Программно-аппаратные способы защиты информационной системы аэропорта

- eToken (electronic token) – электронный ключ, являющийся средством аутентификации и защищенного хранения информации в качестве цифровой подписи.
 - Secret Disk – система, защищающая важные данные на устройствах.
 - Сервер мониторинга анализирует информацию о состоянии всех включенных устройств.
 - Агент контроля настроек сетевого оборудования проверяет целостность файлов конфигурации работающих устройств.
 - Сертифицированное средство защиты информации.
- Административные способы защиты информационной системы аэропорта представлены на рис. 3.

Чтобы улучшить защиту информации, обрабатываемой в гражданской авиации, была осуществлена разработка следующих рекомендаций:

- Кругу уполномоченных пользователей, имеющему доступ к ресурсам системы, следует осуществлять безопасное соединение передачи данных, не распространять конфиденциальную информацию по

сторонним, при уходе блокировать доступ к компьютеру.



Рис. 3. Административные способы защиты информационной системы аэропорта

- Необходимо регулярно обновлять антивирусное ПО (программное обеспечение).
- Для безопасного входа в сеть следует установить двухфакторную аутентификацию при ее наличии.
- Важно периодически менять пароль, используемый пользователем.
- Необходимо установить контроль доступа к информационной системе.

Заключение

Серьезными угрозами системы обработки информации аэропорта являются в равной степени и противоправные действия сотрудников, и взламывания правонарушителями корпоративной сети. Чтобы уменьшить риски несанкционированной аутентификации в информационную систему аэропорта, сотрудникам стоит применять программно-аппаратные и административные способы защиты информации. Существует множество рекомендации о том, как обеспечить безопасность корпоративных систем, однако злоумышленники придумывают новые способы взлома информационных систем, поэтому следует регулярно улучшать способы защиты информации в гражданской авиации.

Список литературы

1. **Мельников В.П.** Информационная безопасность и защита информации: учебное пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков – М.: Академия, 2008. – 336 с.
2. **Духан Е.И.** Программно-аппаратные средства защиты компьютерной информации. Практический курс: учеб. пособие / Е.И. Духан, Н.И. Синадский, Д.А. Хорьков – Екатеринбург: УрГУ, 2008. – 240 с.
3. **Внуков А.А.** Защита информации: учеб. пособие / А.А. Внуков – М.: Юрайт, 2018. – 261 с.

РАЗРАБОТКА АЛГОРИТМА ОПТИМИЗАЦИИ ИГРОВОГО ПРОЕКТА ПРИ ПОМОЩИ ШАБЛОНА ПРОЕКТИРОВАНИЯ ОБЪЕКТ POOL



Алтунин Андрей Владимирович

Студент 4-го курса Государственного технологического университета «СТАНКИН»



Бритвина Валентина Валентиновна

Кандидат педагогических наук, доцент кафедры «Управление и информатика в технических системах» Московского государственного технологического университета «СТАНКИН», доцент кафедры «Инфокогнитивные технологии» Московского политехнического университета

Аннотация. В статье рассмотрены различные способы оптимизации игровых проектов. В рамках рассмотренных способов, разработан и внедрен собственный алгоритм оптимизации, основанный на шаблоне проектирования object pool.

Ключевые слова: информационные технологии, оптимизация, игровые объекты, алгоритм.

Annotation. The article discusses various ways to optimize game projects. Within the considered methods, developed and implemented its own optimization algorithm based on the design pattern object pool.

Keywords: information technology, optimization, game objects, algorithm.