**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Петербургский государственный университет путей сообщения**

**Императора Александра I»**

**(ФГБОУ ВО ПГУПС)**

Факультет «Автоматизация и интеллектуальные технологии»

Кафедра «Информатика и информационная безопасность»

Лабораторная работа № 2

по дисциплине

«Информационная безопасность автоматизированных транспортных систем»

«Классификация корпоративной автоматизированной системы или сети по требованиям безопасности информации»

|  |  |  |
| --- | --- | --- |
| **Выполнили обучающиеся**  Курс 5  Группа КИБ-012 |  | Г.Е. Груздев |
|  |  |  |
| **Проверил** |  | А.А. Корниенко |

Санкт-Петербург

2024

# Задание

***Цель выполнения лабораторной работы:***

Изучение требований нормативных документов по безопасности информации для автоматизированных систем и овладение навыками анализа угроз и уязвимостей информационной безопасности и оценивания защищенности автоматизированных и информационно-управляющих системах на транспорте.

***Задание:***

Изучить руководящие документы ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» и «Специальные требования и рекомендации по технической защите конфиденциальной информации».

Провести классификацию выбранной корпоративной автоматизированной системы или сети на основании руководящего документа ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Оценить соответствие подсистемы защиты информации выбранной корпоративной автоматизированной системы или сети (АС) по требованиям безопасности информации указанных нормативных документов.

# КРАТКОЕ ОПИСАНИЕ АРХИТЕКТУРЫ И ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ВЫБРАННОЙ КОРПОРАТИВНОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ИЛИ СЕТИ.

ДИСПАРК - Автоматизированная система полномерного учета, контроля дислокации, анализа использования и регулирования вагонного парка на железных дорогах России.

Система ДИСПАРК предназначена для: формирования объективных данных о наличии и состоянии вагонного парка на сети, железных дорогах, обеспечения сохранности вагонного парка РФ.

ДИСПАРК создан в целях достижения максимальной прибыли железных дорог за счет полного удовлетворения заявок грузовладельцев на перевозку с минимальными эксплуатационными расходами по их обеспечению.

ДИСПАРК является одним из важнейших комплексов информационных технологий и включает три уровня:

1. сетевой (ГВЦОЛО «РЖД»); Сетевой уровень системы ДИСПАРК реализуется на базе вагонной модели ГВЦ ОАО «РЖД» в увязке с цен тральной картотекой электронных паспортов вагонов (ЦКПВ).
2. дорожный (ИВЦ ж.д.). Дорожный уровень ДИСПАРК-2 реализуется как часть общей системы упр-я грузовыми пер-ми железных дорог (АСУ ГП ж.д.), на современных ГПК
3. линейный (локальные сети и отдельные АРМ на базе ПК для работы в линейных предприятиях), с постепенным преобразованием линейных систем в комплексы АРМ пользователей, работающих напрямую с дорожными базами данных.

База данных ДИСПАРК строится поездной (ПМД), отправочной (ОМД) и вагонной модели дороги. Основными пользователями системы являются работники служб движения, коммерческой работы.

Система ДИСПАРК создавалась поэтапно:

1. Первый этап – оздоровление парка и пономерной контроль за его содержанием, что является одной из главных целей создания системы.
2. Второй этап – слежение за каждым вагоном, где бы он не находился, в составе поезда, на станционных путях, а также за всеми операциями, которые выполняются с вагоном в пути следования. На втором этапе, кроме этого, была создана база данных о вагоне с очень высокой степенью дислокации сведений по техническим, технологическим и географическим признакам в реальном масштабе времени.
3. Третий этап связан с преобразованием методов упр-я экспл-й работой в целом, в первую очередь на дорожном уровне.
4. Функции четвертого этапа связаны с коренным преобразованием существующей системы подготовки и перемещения пер-х документов и создания на этой основе более гибко, достоверной и мобильной системы расчетов за выполненные перевозки.

Кроме функций учета, контроля, анализа, реализации диалоговых процедур и мотивации управляющих воздействий, сформированы функции оперативного прогнозирования производственных ситуаций и дорожно-сетевых сценариев работы вагонного парка на ближайшее время, на несколько суток вперед, а также методы оптимального регулирования погрузочных ресурсов.

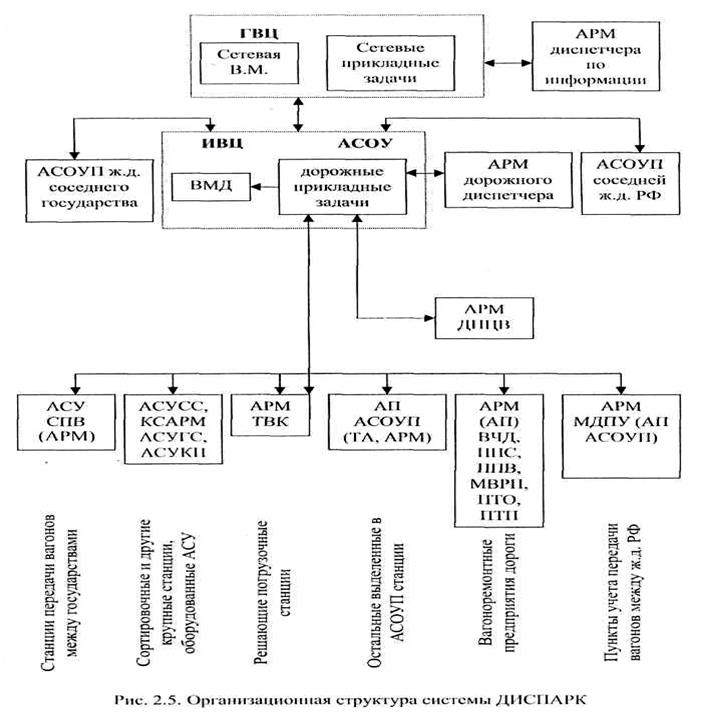


Рисунок 1 – Организационная структура системы ДИСПАРК

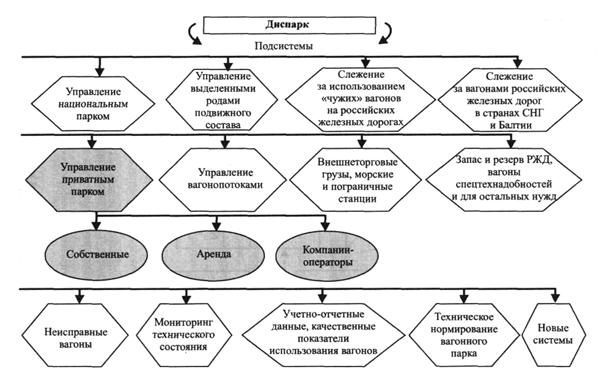


Рисунок 2 – Подсистемы ДИСПАРК

# ИСХОДНЫЕ ДАННЫЕ ДЛЯ ПРОВЕДЕНИЯ КЛАССИФИКАЦИИ АС

Исходными данными для проведения классификации будем считать информационные ресурсы и элементы архитектуры, подлежащие защите.

Исходя из списка элементов структуры ДИСПАРК, к защищаемым элементам инфраструктуры и защищаемым активам относятся:

1. Информационные ресурсы:

* База данных поездной модели дороги (ПМД).
* База данных отправочной модели дороги (ОМД).
* База данных вагонной модели дороги.
* Центральная картотека электронных паспортов вагонов (ЦКПВ).
* Информация о технических, технологических и географических характеристиках вагонов.
* Данные о местоположении вагонов и выполняемых операциях в реальном времени.
* Прогнозные данные производственных ситуаций и сетевых сценариев работы вагонного парка.

2. Элементы архитектуры системы:

2.1 Сетевой уровень:

* Инфраструктура ГВЦОЛО «РЖД».
* Серверные мощности для хранения и обработки данных на сетевом уровне.
* Системы вагонной модели ГВЦ.

2.2 Дорожный уровень:

* Информационно-вычислительные центры железных дорог (ИВЦ ж.д.).
* Модуль управления грузовыми перевозками (АСУ ГП ж.д.).

2.3 Линейный уровень:

* Локальные сети предприятий.
* Автоматизированные рабочие места (АРМ) пользователей, работающие с дорожными базами данных.

3. Инфраструктурные активы:

* Серверы, хранилища данных и сетевое оборудование (маршрутизаторы, коммутаторы, сетевые шлюзы).
* Программное обеспечение, используемое для управления данными (системы управления базами данных, аналитические модули).
* Системы обеспечения безопасности, включая межсетевые экраны и системы обнаружения вторжений.
* Коммуникационные каналы для обмена данными между уровнями архитектуры.
* Резервные копии баз данных и системы аварийного восстановления.

4. Организационные активы:

* Регламенты и процедуры работы с системой.
* Логины и пароли пользователей (аутентификационные данные).
* Журналы и записи аудита операций с данными.
* Права доступа и политики разграничения доступа.

5. Физические активы:

* Серверные помещения с обеспечением физической безопасности.
* Устройства ввода-вывода информации (рабочие станции, терминалы).

# ОПРЕДЕЛЕНИЕ КЛАССА АС С ОБОСНОВАНИЕМ

Система ДИСПАРК является многопользовательской автоматизированной системой (АС), в которой одновременно обрабатывается и хранится информация различных уровней конфиденциальности.

**1. Обоснование выбора группы АС**

С учетом организационной структуры системы:

* Доступ к данным имеют различные пользователи (диспетчеры, сотрудники служб движения и коммерческой работы).
* Права доступа дифференцированы: каждый пользователь имеет доступ только к информации, необходимой для выполнения своих задач.
* Ограничивается доступ сотрудников к секретной информации в зависимости от их полномочий.

**Группа:** *Первая группа АС* (многопользовательские системы с разными полномочиями на доступ к конфиденциальной информации).

2. Обоснование выбора класса АС

В системе ДИСПАРК обрабатывается информация следующих уровней конфиденциальности:

**Секретная информация:**

* Сведения, относящиеся к оперативной организации перевозок вагонного парка.
* Ущерб от раскрытия таких данных может затронуть интересы транспортной отрасли, экономической безопасности и логистических процессов Российской Федерации.

**Информация ограниченного доступа:**

* Технические, технологические и географические данные о вагонном парке.
* Раскрытие может привести к нарушению работы перевозок и интересов ОАО «РЖД».

Так как в системе обрабатываются секретные данные и информация ограниченного доступа, в соответствии с РД классификация определяется между классами 1Г и 1В.

**Класс 1Г:** Предназначен для многопользовательских АС, обрабатывающих данные ограниченного доступа.

**Класс 1В:** Предназначен для многопользовательских АС, в которых обрабатывается секретная информация (в том числе государственная тайна).

**3. Окончательный выбор класса АС для системы ДИСПАРК**

Учитывая, что:

* Нет государственной тайны.
* Система отвечает за бесперебойную организацию перевозок, что делает ее критическим элементом инфраструктуры.

**Системе ДИСПАРК присваивается класс защищенности 1Г.**

# ПРОВЕРКА АС СООТВЕТСТВИЯ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Основываясь на классификации системы ДИСПАРК как автоматизированной системы первого класса (1Г), определим существующие меры и средства защиты информации, а также объекты инфраструктуры, подлежащие защите.

Основные объекты защиты для системы ДИСПАРК

1. **Информационные ресурсы:**

* База данных вагонной модели, содержащая данные о местоположении, состоянии и использовании вагонного парка.
* Данные электронных паспортов вагонов (ЦКПВ).
* Оперативные данные о состоянии сети железных дорог и перевозок.
* Данные о планировании и прогнозировании эксплуатационных сценариев.

1. **Инфраструктурные элементы:**

* Серверы сетевого уровня (ГВЦОЛО ОАО «РЖД»).
* Серверы дорожного уровня (ИВЦ ж.д.).
* Локальные рабочие станции и АРМ (автоматизированные рабочие места) линейного уровня.
* Сетевые каналы связи между уровнями системы.
* Системы хранения данных (поездная, отправочная и вагонная модели).

1. **Технологические процессы:**

* Процессы мониторинга и управления вагонным парком.
* Процессы учета и анализа производственных ситуаций.
* Регулирование погрузочных ресурсов.

1. **Пользователи системы:**

* Диспетчеры служб движения.
* Сотрудники коммерческой службы.
* Администраторы системы.

**Требования к мерам защиты информации**

1. **Идентификация и аутентификация пользователей:**

* Использование уникальных учетных записей и паролей.
* Внедрение двухфакторной аутентификации для пользователей с доступом к конфиденциальной информации.

1. **Разграничение прав доступа:**

* Настройка прав доступа в зависимости от функциональных обязанностей пользователя.
* Ограничение доступа к секретной информации только для уполномоченных лиц.

1. **Контроль целостности данных:**

* Использование хэш-функций для проверки целостности информации.
* Регулярный аудит данных баз системы.

1. **Защита каналов связи:**

* Шифрование данных при передаче через сеть с использованием современных криптографических алгоритмов (например, TLS).
* Внедрение VPN для удаленного доступа к системе.

1. **Защита хранимой информации:**

* Использование шифрования данных на серверах и рабочих станциях.
* Резервное копирование данных с возможностью восстановления.

1. **Мониторинг и управление событиями безопасности:**

* Установка систем мониторинга событий безопасности (SIEM).
* Логирование действий пользователей и системных событий.
* Анализ журналов безопасности для выявления подозрительной активности.

1. **Обнаружение и предотвращение атак:**

* Установка систем обнаружения и предотвращения вторжений (IDS/IPS).
* Обновление и поддержка антивирусного ПО.

1. **Физическая защита:**

* Ограничение доступа к серверным помещениям и местам хранения оборудования.
* Использование видеонаблюдения и систем контроля доступа.

1. **Обучение и осведомленность пользователей:**

* Проведение регулярного обучения сотрудников в области информационной безопасности.
* Ознакомление с политиками и процедурами работы с конфиденциальной информацией.

Для проверки соответствия системе ДИСПАРК требованиям информационной безопасности необходимо:

1. Провести аудит действующих мер защиты информации.
2. Сравнить текущие меры с требованиями для систем класса 1Г, установленными нормативными документами.
3. Определить пробелы и разработать план их устранения.
4. Внедрить недостающие меры защиты и провести повторную проверку.

# ВЫВОД

По результатам проведенной классификации системе ДИСПАРК присвоен класс 1Г. Классификация осуществлена на основании анализа архитектуры системы ДИСПАРК, информационных ресурсов и элементов критической инфраструктуры, подлежащих защите.

Анализ существующих мер защиты показал, что система ДИСПАРК соответствует требованиям обеспечения защиты информации, предъявляемым к системам класса 1Г.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ:

1. Руководящий документ Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации".
2. Информационная безопасность и защита информации на железнодорожном транспорте: учебник: в 2ч. / С.Е. Адауров и др.; под ред. А.А. Корниенко. - М.: ФГБОУ "Учебно-методический центр по образованию на железнодорожном транспорте", 2014.
3. ФЗ № 5485-1 от 21 июля 1993 года "О государственной тайне".
4. Телемеханические системы управления движением поездов : учеб. пособие / А. Д. Манаков. – Хабаровск : Изд-во ДВГУПС, 2005. – 55 с.
5. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: учебник для вузов ж.-д. транспорта. / В.В. Яковлев, А.А. Корниенко — М.: УМК МПС России, 2002. — 328 с.