kaspersky

Техническая документация

Модуль безопасности для автономного робота-уборщика, устойчивого к киберугрозам на основе методов конструкций безопасности.

КОМАНДА

"HP Laser MFP 125w"

Международный хакатон 2025

г. Санкт-Петербург
2025 г.

Оглавление

Введение

Назначение документа

Данное руководство предназначено для администраторов и разработчиков системы защиты от киберпрепятствий роботизированной платформы. В нем содержатся сведения, необходимые для ознакомления с принципами работы, архитектурой и возможностями применения системы защиты.

Область применения

Система защиты предназначена для обеспечения кибербезопасности автономных роботизированных платформ при выполнении задач навигации и управления в условиях воздействия киберпрепятствий. Система может применяться в различных областях, включая промышленную автоматизацию, логистику и специальные применения.

Термины и определения

В документе используются следующие основные термины:

Киберпрепятствие (CybP) - преднамеренное воздействие на систему управления роботизированной платформой с целью нарушения ее нормального функционирования

UserMissionHandler - модуль выполнения миссии, отвечающий за навигацию и управление движением

UserTrustedHandler - модуль безопасности, реализующий механизмы защиты от киберпрепятствий

Автопилот - программный модуль, обеспечивающий автономное движение по заданному маршруту

Контроль целостности - механизм проверки неизменности программных компонентов системы

Глава 1
Общие сведения

Назначение системы

Назначение системы

Система защиты от киберпрепятствий предназначена для обеспечения кибербезопасности роботизированных платформ, функционирующих в автономном режиме. Система обеспечивает защиту от шести типов киберпрепятствий (CybP_01 - CybP_06) и гарантирует непрерывность выполнения задач в условиях кибератак.

Система разработана для работы в реальном времени и должна обеспечивать минимальное время реакции на кибератаки.

Система обеспечивает:

- защиту систем управления от несанкционированного вмешательства;
- контроль целостности программных компонентов;
- мониторинг состояния оборудования в реальном времени;
- автоматическое восстановление после кибератак.

Основные функции

Система защиты реализует следующие основные функции:

- Управление движением по заданному маршруту
- Визуальная детекция и распознавание объектов
- Перехват и анализ сетевого трафика (UDP)
- Взаимодействие с системами управления движением
- Контроль состояния навесного оборудования
- Мониторинг целостности автопилота (CybP_01)
- Защита от подмены сообщений (CybP_02)
- Мониторинг состояния приводов (CybP_03)
- Контроль скорости щетки (CybP_04)
- Защита систем управления шлагбаумом (CybP_05)
- Контроль скорости движения (CybP_06)
- Функциональный контроль защитных подсистем
- Самозащита от несанкционированных воздействий
- Централизованный сбор и анализ журналов событий
- Визуализация состояния системы в реальном времени
- Автоматическое применение защитных мер
- Уведомление оператора о критических событиях

Состав компонентов системы

Система защиты состоит из следующих программных компонентов:

1. Модуль выполнения миссии (UserMissionHandler)
2. Модуль безопасности (UserTrustedHandler)
3. Система коммуникации

Назначение компонентов

Модуль выполнения миссии

Обеспечение выполнения основной задачи роботизированной платформы - движение по маршруту с преодолением препятствий. Данный модуль является основным исполнительным компонентом системы, отвечающим за выполнение поставленной задачи.
Модуль функционирует в реальном времени и обеспечивает:

- Планирование и выполнение маршрута движения
- Обработку данных с датчиков и камер
- Взаимодействие с внешними устройствами (светофоры, шлагбаумы)
- Управление скоростью и направлением движения

Модуль безопасности

Реализация механизмов защиты от киберпрепятствий и обеспечение безопасного функционирования платформы. Модуль безопасности обеспечивает защиту системы от киберпрепятствий и функционирует параллельно с основным модулем.

Основные функции:

- Непрерывный мониторинг состояния системы
- Обнаружение и нейтрализация кибератак
- Восстановление работоспособности после атак
- Ведение журнала событий безопасности

Система коммуникации

Обеспечивает надежное взаимодействие между компонентами системы и внешними устройствами:

- Обмен сообщениями между модулями
- Передачу данных по сетевых протоколам
- Синхронизацию работы компонентов
- Резервирование каналов связи

Глава 2
Составные части

Группы функциональных компонентов

Система защиты от киберпрепятствий состоит из двух основных функциональных групп компонентов:

- Модуль выполнения миссии (UserMissionHandler) - базовый исполнительный компонент
- Модуль безопасности (UserTrustedHandler) - защитный компонент

Подключаемые функциональные компоненты

- Локальная защита - механизмы защиты оборудования и систем управления
- Сетевая защита - механизмы защиты сетевого взаимодействия
- Защита от киберпрепятствий - специализированные механизмы противодействия CybP

Модуль выполнения миссии (UserMissionHandler)

Модуль выполнения миссии является основным исполнительным компонентом системы, отвечающим за выполнение задач автономной навигации и управления роботизированной платформой.

Состав модуля:

- Ядро выполнения миссии
- Подсистема управления движением
- Подсистема компьютерного зрения
- Подсистема сетевого взаимодействия
- Подсистема управления оборудованием

Модуль безопасности (UserTrustedHandler)

Модуль безопасности обеспечивает защиту роботизированной платформы от киберпрепятствий через непрерывный мониторинг, обнаружение атак и автоматическое применение защитных мер.

Состав модуля:

- Ядро безопасности
- Подсистема мониторинга целостности (CybP_01)
- Подсистема защиты сообщений (CybP_02)
- Подсистема мониторинга приводов (CybP_03)
- Подсистема контроля оборудования (CybP_04)
- Подсистема защиты шлагбаума (CybP_05)
- Подсистема контроля скорости (CybP_06)
- Подсистема регистрации событий

Глава 3
Механизмы защиты

Система защиты обеспечивает противодействие шести типам киберпрепятствий, классифицированных по уровню критичности:

Уровень угрозы	Тип Киберпрепятсвия	Наименование
ВЫСОКИЙ	CybP_01	Компрометация автопилота
СРЕДНИЙ	CybP_02	Подмена сообщений
СРЕДНИЙ	CybP_03	Компрометация приводов
НИЗКИЙ	CybP_04	Сбой навесного оборудования
НИЗКИЙ	CybP_05	Компрометация шлагбаума
СРЕДНИЙ	CybP_06	Несанкционированное ускорение

Защита от компрометации автопилота

Киберпрепятствие CybP_01 представляет собой атаку на целостность программного обеспечения автопилота. Механизм атаки заключается в подмене хеш-суммы исполняемого кода системы управления, что приводит к несанкционированной модификации алгоритмов навигации и управления движением. Атака активируется при нахождении роботизированной платформы в триггерных зонах, соответствующих ячейкам 11 и 29 карты движения.

Система защиты реализует многоуровневый механизм противодействия, включающий непрерывный мониторинг целостности кода автопилота с периодичностью 500 миллисекунд. При обнаружении изменения хеш-суммы система автоматически инициирует процедуру восстановления, которая включает сброс автопилота и ожидание восстановления исходного состояния в течение не более 10 секунд. В критических случаях применяется экстренная остановка системы с обязательным уведомлением оператора.

Защита от подмены сообщений

Киберпрепятствие CybP_02 характеризуется внедрением несанкционированных сообщений в систему межмодульного взаимодействия. Атака проявляется в виде подмены легитимных сообщений между компонентами системы или внедрения специально сформированных "жалобных" сообщений, имитирующих системные уведомления. Всего система детектирует 30 типов подобных сообщений, включая характерные фразы типа "Снова эта работа..." или "Я мог бы вычислять траектории звезд."

Механизм защиты основан на многоуровневой верификации всех передаваемых сообщений, включая контроль формата, содержания, отправителя и временных меток. Система осуществляет фильтрацию сетевого трафика с блокировкой сообщений, содержащих запрещенные паттерны, и ведет постоянное ведение черного списка подозрительных источников. При обнаружении попыток подмены система автоматически генерирует корректные защищенные сообщения и восстанавливает нарушенные каналы коммуникации.

Защита от компрометации приводов

Киберпрепятствие CybP_03 направлено на нарушение работы системы управления приводами роботизированной платформы. Атака осуществляется через подмену данных в каналах управления приводами, где в поле last_received_from устанавливается значение "eeeeeeee". Это приводит к некорректной работе системы управления движением и потенциальной потере контроля над платформой.

Система защиты обеспечивает непрерывный мониторинг состояния всех приводов с интервалом 100 миллисекунд, что позволяет обнаруживать поддельные данные в реальном времени. При выявлении компрометации автоматически запускается процедура восстановления, включающая сброс скомпрометированного привода и перезагрузку автопилота. В случае критических нарушений система инициирует экстренную остановку с полной блокировкой управления до полного восстановления работоспособности системы.

Защита от сбоя навесного оборудования

Киберпрепятствие CybP_04 проявляется в виде несанкционированного изменения параметров работы навесного оборудования, в частности - скорости вращения щетки. Атака приводит к превышению допустимых параметров работы оборудования, что может вызвать его преждевременный износ или нарушение выполнения основных функций.

Система защиты осуществляет постоянный мониторинг скорости щетки с установленной нормальной скоростью 100 единиц и порогом обнаружения атаки 150 единиц. Контроль производится с периодичностью 500 миллисекунд. При обнаружении превышения допустимых параметров система автоматически выполняет коррекцию настроек через сброс контроллера скорости и восстановление нормальных рабочих параметров. Дополнительно ведется статистика работы оборудования для раннего обнаружения аномалий.

Защита от компрометации шлагбаума

Киберпрепятствие CybP_05 представляет собой атаку на систему управления шлагбаумом, проявляющуюся в блокировке изменения его состояния или подмене управляющих команд. Это препятствует нормальному прохождению маршрута роботизированной платформой и может привести к срыву выполнения миссии.

Система защиты реализует мультиметодный подход к верификации состояния шлагбаума, используя одновременно компьютерное зрение для визуального контроля и анализ UDP-трафика на порту 15000 для проверки сетевых команд. При обнаружении расхождений между ожидаемым и фактическим состоянием система предпринимает многократные попытки коррекции управления, а в случае persistentных проблем обеспечивает возможность ручного вмешательства оператора.

Защита от несанкционированного ускорения

Киберпрепятствие CybP_06 характеризуется принудительным увеличением скорости движения роботизированной платформы сверх установленных допустимых пределов. Атака активируется в определенных триггерных зонах (ячейки 62, 71, 31, 40) и представляет серьезную угрозу безопасности движения.

Система защиты осуществляет непрерывный расчет текущей скорости на основе анализа изменения позиции платформы с использованием формулы вычисления расстояния между последовательными координатами. При нормальной скорости 0.24 м/с порог обнаружения атаки установлен на уровне 0.35 м/с. Мониторинг производится с интервалом 500 миллисекунд. При обнаружении несанкционированного ускорения система автоматически применяет принудительное ограничение скорости и блокирует команды, приводящие к превышению допустимых параметров движения.

Применяемые фукнции

Защита от компрометации автопилота:

Функции мониторинга:

- *_start_autopilot_monitoring* - запуск мониторинга автопилота
- *_initialize_original_hash* - инициализация эталонного хеша
- *_check_autopilot_integrity* - проверка целостности кода автопилота

Функции восстановления:

- *_apply_cybp01_protection* - применение защиты
- *_wait_for_autopilot_recovery* - ожидание восстановления
- *_handle_cybp01_recovery* - обработка успешного восстановления

Аварийные функции:

- *_apply_emergency_stop_cybp01* - экстренная остановка
- *_reset_cybp01_state* - сброс состояния защиты

Защита от подмены сообщений

Основные функции:

- *make_next_short_message* - генерация защищенных сообщений
- *_detect_cybp02_attack* - обнаружение атаки подмены сообщений

Защита от компрометации приводов

Функции мониторинга:

- *cybp03_start_drive_monitoring* - запуск мониторинга приводов
- *cybp03_check_drive_integrity* - проверка целостности данных приводов
- *cybp03_detect_attack* - обнаружение атаки на приводы

Функции восстановления:

- *cybp03_apply_protection* - применение защиты
- *cybp03_attempt_drive_reset* - попытка сброса привода
- *cybp03_wait_for_recovery* - ожидание восстановления

Защита от сбоя навесного оборудования

Основные функции:

- *_start_brush_monitoring* - запуск мониторинга щетки
- *_check_brush_speed* - контроль скорости щетки
- *_handle_cybp04_attack* - обработка атаки на щетку
- *_apply_cybp04_protection* - применение защиты
- *_verify_protection_applied* - верификация применения защиты
- *_handle_cybp04_recovery* - восстановление после атаки

Защита от компрометации шлагбаума

Функции проверки:

- *check_CybP_05_CV* - проверка через компьютерное зрение
- *check_CybP_05_UDP* - проверка через UDP-трафик

Функции управления:

- *change_barrier_UDP* - управление шлагбаумом через UDP
- *change_barrier_CV* - управление шлагбаумом через компьютерное зрение

Защита от несанкционированного ускорения

Функции мониторинга:

- *_start_speed_monitoring* - запуск мониторинга скорости
- *_calculate_robot_speed* - расчет скорости движения
- *_check_robot_speed_and_position* - контроль скорости и позиции
- *_calculate_cell_from_position* - расчет номера клетки из координат

Функции защиты:

- *_handle_cybp06_speed_attack* - обработка атаки превышения скорости
- *_apply_cybp06_speed_protection* - применение защиты

Общие системные функции

Управление мониторингом:

- *_start_all_monitoring_systems* - запуск всех систем мониторинга
- *trusted_code* - основной цикл работы модуля безопасности

Функции перехвата трафика:

- *intercept_UDP* - перехват UDP-трафика устройств
- *check_autobot_UDP* - мониторинг положения автобота

Функции компьютерного зрения:

- *check_t_light_CV* - проверка светофора
- *check_pedestrian_CV* - детекция пешеходов
- *get_photo* - получение данных с камеры

Контактная информация: