|  |  |
| --- | --- |
| **Изображение выглядит как текст, Шрифт, логотип, Графика  Автоматически созданное описание** |  |

КОНКУРСНОЕ ЗАДАНИЕ КОМПЕТЕНЦИИ

«Кибериммунная автономность»

Итогового (Межрегионального) этапа Чемпионата высоких технологий в 2025 г

Новгородская область

регион проведения

2025 г.

Конкурсное задание разработано экспертным сообществом и утверждено Менеджером компетенции, в котором установлены нижеследующие правила и необходимые требования владения профессиональными навыками для участия в соревнованиях по профессиональному мастерству.

**Конкурсное задание включает в себя следующие разделы:**

[1. ОСНОВНЫЕ ТРЕБОВАНИЯ КОМПЕТЕНЦИИ 4](#_Toc201664693)

[1.1. ОБЩИЕ СВЕДЕНИЯ О ТРЕБОВАНИЯХ КОМПЕТЕНЦИИ 4](#_Toc201664694)

[1.2. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ ЗАДАЧ СПЕЦИАЛИСТА ПО КОМПЕТЕНЦИИ «Кибериммунная автономность» 4](#_Toc201664695)

[1.3. ТРЕБОВАНИЯ К СХЕМЕ ОЦЕНКИ 7](#_Toc201664696)

[1.4. СПЕЦИФИКА ОЦЕНКИ КОМПЕТЕНЦИИ 7](#_Toc201664697)

[1.5. КОНКУРСНОЕ ЗАДАНИЕ 9](#_Toc201664698)

[1.5.1. Разработка/выбор конкурсного задания 9](#_Toc201664699)

[1.5.2. Структура модулей конкурсного задания 9](#_Toc201664700)

[2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ 15](#_Toc201664701)

[2.1. Личный инструмент конкурсанта 15](#_Toc201664702)

[2.2. Материалы, оборудование и инструменты, запрещенные на площадке 16](#_Toc201664703)

[2.3. Материалы, предоставляемые конкурсантам: 16](#_Toc201664704)

[2.4. В ходе соревнований конкурсантам разрешается: 17](#_Toc201664705)

[2.5. В ходе соревнований конкурсантам запрещается: 17](#_Toc201664706)

[3. ПРИЛОЖЕНИЯ 17](#_Toc201664707)

**ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ**

1. ФГОС – Федеральный государственный образовательный стандарт
2. ПС – Профессиональный стандарт
3. КЗ – Конкурсное задание
4. ИЛ – Инфраструктурный лист
5. АНТС - автономное наземное транспортное средство

# 1. ОСНОВНЫЕ ТРЕБОВАНИЯ КОМПЕТЕНЦИИ

## 1.1. ОБЩИЕ СВЕДЕНИЯ О ТРЕБОВАНИЯХ КОМПЕТЕНЦИИ

Требования компетенции (ТК) «Кибериммунная Автономность» определяют знания, умения, навыки и трудовые функции, которые лежат в основе наиболее актуальных требований работодателей отрасли.

Целью соревнований по компетенции является демонстрация лучших практик и высокого уровня выполнения работы по соответствующей рабочей специальности или профессии.

Требования компетенции являются руководством для подготовки конкурентоспособных, высококвалифицированных специалистов / рабочих и участия их в конкурсах профессионального мастерства.

В соревнованиях по компетенции проверка знаний, умений, навыков и трудовых функций осуществляется посредством оценки выполнения практической работы.

Требования компетенции разделены на четкие разделы с номерами и заголовками, каждому разделу назначен процент относительной важности, сумма которых составляет 100.

## 1.2. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ ЗАДАЧ СПЕЦИАЛИСТА ПО КОМПЕТЕНЦИИ «Кибериммунная автономность»

*Таблица №1*

**Перечень профессиональных задач специалиста**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Раздел** | **Важность в %** |
| 1 | **Формулировка целей безопасности автономной системы**  - Специалист должен знать и понимать:  Триаду безопасности (Конфиденциальность, Целостность, Доступность),  Ключевые критерии формулировок Целей Безопасности,  Типовые примеры Целей Безопасности.  - Специалист должен уметь:  Анализировать функционал системы и определять ключевые ценности / активы в ней.  Моделировать последствия нарушения Целей безопасности для оценки ущерба  Приоритизировать (с представителями бизнеса) угрозы, ущерб и ценность активов. | 5 |
| 2 | **Определение / выделение критического функционала автономной системы** | 15 |
| - Специалист должен знать и понимать:  Необходимость определения критических функций для достижения заданных целей безопасности  Основы моделирования угроз  Способы графического представления архитектуры системы  Нотацию и назначение политики архитектуры  Методы документирования сценариев атак в формате диаграмм последовательности  Язык markdown для создания текстовой документации |
| - Специалист должен уметь:  Анализировать архитектуру системы и выделять критический программный код и аппаратные ресурсы  Применять различные инструменты диаграммирования для описания сценариев атак и их влияния на цели безопасности  Обосновывать архитектурные решения в формате таблиц принятия решения  Документировать архитектуру решения в формате markdown по образцу |
| 3 | **Внедрение/подключение встраиваемых систем безопасности** | 40 |
| - Специалист должен знать и понимать:  Ключевые особенности встроенных систем безопасности, принципы разделения и контроля взаимодействия  В частности, технологию разделения на домены безопасности и контроль взаимодействия MILS  Технологию и принцип работы мониторов безопасности FLASK |
| - Специалист должен уметь:  Читать схемы разводки плат и соединений  Установить существующий модуль безопасности и дополнительные цепи контроля для обеспечения выполнения критических команд |
| 4 | **Настройка встраиваемых систем безопасности** | 20 |
| - Специалист должен знать и понимать:  Логику и синтаксис определения политик безопасности на уровне модуля безопасности устройства |
| - Специалист должен уметь:  настроить модуль безопасности для реализации заданной политики архитектуры  написать политики безопасности для заданной политики архитектуры на заданном в сценарии соревнований языке программирования |
| 5 | **Верификация работы встраиваемых систем безопасности** | 20 |
| - Специалист должен знать и понимать:  Логику разработки тестов, какие тесты безопасности нужны и почему такие  Особенности автоматизированных модульных тестов  Особенности автоматизированных сквозных тестов  Технологии разработки автоматизированных тестов с использованием таких языков программирования как, например, C/C++, Python, Java, Rust  Требования техники безопасности для осуществления тестовых поездок |
| - Специалист должен уметь:  Написать автоматический тест для проверки работы политик безопасности системы  Написать сквозной автоматический тест для проверки функционирования системы в условиях компрометации встроенных систем (согласно сценарию соревнований)  Запустить разработанные автоматические тесты для проверки систем безопасности на стенде под управлением ОС на базе Linux  Собрать результаты тестирования и подготовить отчёт  Осуществить тестовые поездки конструктивно защищённой машинки с соблюдением заданных ограничений и техники безопасности |

## 

## 1.3. ТРЕБОВАНИЯ К СХЕМЕ ОЦЕНКИ

Сумма баллов, присуждаемых по каждому аспекту, должна попадать в диапазон баллов, определенных для каждого раздела компетенции, обозначенных в требованиях и указанных в таблице №2.

*Таблица №2*

**Матрица пересчета требований компетенции в критерии оценки**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Критерий/Модуль** | | | | | | **Итого баллов за раздел ТРЕБОВАНИЙ КОМПЕТЕНЦИИ** |
| **Разделы ТРЕБОВАНИЙ КОМПЕТЕНЦИИ** |  | **A** | **Б** | **В** | **Г** |  |
| **1** | 0 | 0 | 0 | 4 | 4 |
| **2** | 0 | 12 | 6 | 0 | 18 |
| **3** | 16 | 0 | 0 | 22 | 38 |
| **4** | 0 | 2 | 6 | 8 | 16 |
| **5** | 0 | 8 | 8 | 8 | 24 |
| **Итого баллов за критерий/модуль** | | 16 | 22 | 20 | 42 | **100** |

## 1.4. СПЕЦИФИКА ОЦЕНКИ КОМПЕТЕНЦИИ

Оценка Конкурсного задания будет основываться на критериях, указанных в таблице №3:

*Таблица №3*

**Оценка конкурсного задания**

|  |  |  |
| --- | --- | --- |
| **Критерий** | | **Методика проверки навыков в критерии** |
| **А** | **Сборка автономного устройства** | Во время выполнения модуля конкурсант может самостоятельно проверить, что в его решении:   * необходимые компоненты подключены и запускаются вместе, * компоненты обмениваются данными через передачу сообщений, * устройство способно проехать простейшую трассу (например, точка А->точка Б по прямой).   Результаты выполнения модуля (созданный программный код) оцениваются на предмет:   * наличия / отсутствия ошибок в коде, * полноты подключения всех компонент в соответствии с Заданием, * полноты реализации заданных потоков данных в соответствии с Заданием, * успешного прохождения простейшей трассы, * эффективности разработанного кода. |
| **Б** | **Подготовка и прохождение маршрута без киберпрепятствий** | Во время выполнения модуля конкурсант может самостоятельно проверить, что в его решении:   * АНТС проходит необходимый маршрут.   Результаты выполнения модуля (созданный программный код) оцениваются на предмет:   * наличия / отсутствия ошибок в коде, * корректное использование индустриальных инструментов планирования маршрута (APMPlanner, MissionPlanner, формат WPL) * корректности прохождения нужной трассы, соблюдение всех ограничений * эффективности разработанного кода. |
| **В** | **Внедрение и настройка блоков безопасности** | Во время выполнения модуля конкурсант может самостоятельно проверить, что в его решении:   * необходимые компоненты защиты подключены и запускаются, * устройство способно выполнить все штатные действия * устройство способно заблокировать попытку выполнить действия, нарушающие Цели Безопасности.   Результаты выполнения модуля (созданный программный код) оцениваются на предмет:   * наличия / отсутствия ошибок в коде, * полноты подключения всех компонент защиты в соответствии с Заданием, * полноты выполнения устройством всех штатных действий, * полноты блокировки устройством всех попыток выполнить действия, нарушающие Цели Безопасности, * эффективности разработанного кода. |
| **Г** | **Прохождение автономной системой трассы с кибер-препятствиями** | Во время выполнения модуля конкурсант может самостоятельно проверить, что в его решении:   * необходимые компоненты защиты подключены и запускаются, * устройство способно выполнить все штатные действия для прохождения трассы * устройство способно заблокировать все кибер-препятствия - возникающие в процессе прохождения трассы попытки выполнить действия, нарушающие Цели Безопасности.   Результаты выполнения модуля (созданный программный код) оцениваются на предмет:   * наличия / отсутствия ошибок в коде, * полноты блокировки устройством всех попыток выполнить действия, нарушающие Цели Безопасности (кибер-препятствий) * скорости и точности прохождения устройством необходимой трассы, * эффективности разработанного кода. |

## 1.5. КОНКУРСНОЕ ЗАДАНИЕ

Общая продолжительность Конкурсного задания[[1]](#footnote-1): 18 ч.

Количество конкурсных дней: 3 дня

Вне зависимости от количества модулей, КЗ должно включать оценку по каждому из разделов требований компетенции.

Оценка знаний конкурсанта должна проводиться через практическое выполнение Конкурсного задания. В дополнение могут учитываться требования работодателей для проверки теоретических знаний / оценки квалификации.

### 1.5.1. Разработка/выбор конкурсного задания

Конкурсное задание состоит из 4-х модулей, включает обязательную к выполнению часть (инвариант) – 4 модуля. Общее количество баллов конкурсного задания составляет 100.

### 1.5.2. Структура модулей конкурсного задания

**Описание задания**

Забота о человеческой жизни всегда была и остаётся главной задачей для общества. С появлением новых технологий Четвёртой промышленной революции люди всё чаще начинают использовать роботов и умные системы. Они помогают работать быстрее, уменьшают влияние ошибок человека и берут на себя опасные задачи. Одно из главных преимуществ таких систем — то, что они могут самостоятельно проводить спасательные операции и тем самым защищать жизни людей.

Конкурсное задание основано на реальном сценарии использования роботизированного пожарного комплекса. Его основная функция — автономное тушение пожара в городской среде и лесопарковой зоне. Успешное выполнение миссии требует обеспечения комплексной безопасности. На работу автопилота могут повлиять как сбои верхнеуровневой логики управления АНТС, так и попытки внешнего вмешательства, такие как кибератака. Главной задачей конкурсантов соревнований станет запрограммировать и интегрировать программные решения в кибериммунный модуль, отвечающий за безопасное выполнение поставленных задач и предотвращающий нештатное поведение робота.

Конкурсантам необходимо создать автономное транспортное средство (АНТС), устойчивое к кибератакам с помощью специального «модуля безопасности». Этот модуль представляет собой дополнительный микрокомпьютер, который независимо от автопилота управляет ключами (реле), встроенными в цепи питания приводов и исполнительных устройств. Транспортное средство является пожарной машиной, которой необходимо в автономном режиме проехать по маршруту до точки пожара и потушить возгорание, не нарушив при этом целей безопасности. Контролируя исполнительные устройства, «модуль безопасности» должен уберечь АНТС от аварий и различных инцидентов, связанных с безопасностью самого транспортного средства и окружающих. Кибератаки и неисправности, которые предстоит побороть конкурсантам: несанкционированное движение робота, сход с маршрутного задания, взаимодействие со шлагбаумом, начало несанкционированного тушения.

На полигоне (рис. 1) присутствует объединенная точка старта и финиша, откуда АНТС начинает и заканчивает свое движение. Целевая точка – это место на трассе, где произошел пожар. Эти точки на протяжении всего конкурсного задания остаются зафиксированными и не меняются. Движение осуществляется по дороге.



Рисунок 1. Трасса для выполнения конкурсного задания

Шлагбаум является интерактивным элементом инфраструктуры. Открытие шлагбаума подразумевается только в случае, если соответствующая команда была передана АНТС через беспроводную сеть. В ином случае АНТС продолжит прохождение маршрута через закрытый шлагбаум и снесет ограждение.

**Цели безопасности**

Устойчивость кибериммунных систем к атакам выражается в том, что поставленные цели безопасности (далее – ЦБ) не нарушаются даже в условиях кибератак (снаружи и изнутри). Для АНТС предъявлены следующие ЦБ:

1. При любых обстоятельствах АНТС осуществляет перемещение в пределах заданных ограничений (только проезжая часть дорог);
2. При любых обстоятельствах АНТС выполняет только аутентичный (подлинный) маршрут, подтверждённый Диспетчером;
3. При любых обстоятельствах АНТС должен избегать столкновений с препятствиями на трассе и с объектами, окружающими трассу;
4. При любых обстоятельствах АНТС осуществляет тушение пожара только в заданной точке и в заданном направлении, а также не более 15 сек.

**Предположения безопасности**

Разработчиками программного обеспечения кибериммуного модуля (конкурсантам Чемпионата) согласованы следующие предположения безопасности (далее – ПБ) – утверждения о смежных системах, которые снимают с разработчиков часть задач для обеспечения ЦБ:

1. Только авторизованный персонал имеет физический доступ к критическим узлам АНТС (то есть исполнительные устройства, устройства навигации и каналы связи не могут быть скомпрометированы и четко исполняют команды автопилота и модуля безопасности);
2. Модуль безопасности также является доверенным с аппаратной точки зрения, согласно пункту ПБ № 1;
3. Только авторизованные операторы имеют доступ к системе планирования заданий;
4. Авторизованные операторы обладают необходимой квалификацией и являются благонадёжными (то есть не имеют намерений причинить ущерб системе или третьим лицам, используя доступ к АНТС).

**Задача конкурсантов**

Конкурсанты получают доступ к необходимым программным модулям и командаВысом для автопилота и кибериммунного модуля, с помощью которых создают программное обеспечение для борьбы с кибератаками.

В рамках одной кибератаки может происходит несколько инцидентов. Каждому возможному инциденту присваивается один из уровней критичности:

* кий;
* Средний;
* Низкий.

Во время выполнения маршрутного задания, конкурсанты столкнутся со следующими сценариями взломов (кибератак):

**Модуль А. Сборка автономного устройства *(Инвариант)***

*Время выполнения модуля: 3 часа*

В процессе выполнения миссии необходимо сверять маршрутное задание, полученное от автопилота с заданием, полученным от Оператора, и запретить движение АНТС при обнаружении несоответствия.

Также, работа АНТС должна начинаться только после получения разрешения от Диспетчера, и приостанавливаться при отзыве разрешения.

Возможные инциденты:

1.1. Выполнение неверной миссии (уровень критичности: высокий)

1.2. Движение без разрешения от Диспетчера (уровень критичности: средний).

**Модуль Б. Подготовка и прохождение маршрута без киберпрепятствий *(Инвариант)***

*Время выполнения модуля: 4 часа*

В процессе выполнения миссии автопилот может ошибиться (сам или с помощью злоумышленников) и инициировать движение к неверной точке. Модуль безопасности должен сопоставлять реальные перемещения робота с аутентичным маршрутом и предотвращать некорректное поведение АНТС.

Возможные инциденты:

2.1. Движение по дороге к неверной точке (уровень критичности: средний)

2.2. Частичный съезд с дороги (на трассе находятся 2 из 3 колёс АНТС) (уровень критичности: низкий)

2.3. Полный съезд с дороги (на трассе находятся 1 или 0 из 3 колёс АНТС) (уровень критичности: средний)

2.4. Столкновение с другими элементами полигона (касание элемента полигона) (уровень критичности: высокий)

**Модуль В. Внедрение и настройка блоков безопасности *(Инвариант)***

*Время выполнения модуля: 2 часа*

При приближении к шлагбауму робот должен остановиться и послать запрос Диспетчеру на открытие шлагбаума. Возобновить движение можно только после получения подтверждения от Диспетчера о том, что шлагбаум открыт.

Возможные инциденты:

3.1. Касание шлагбаума (уровень критичности: низкий)

3.2. Сбивание шлагбаума (уровень критичности: высокий)

**Модуль Г. Прохождение автономной системой трассы с кибер-препятствиями *(Инвариант)***

*Время выполнения модуля: 9 часов*

АНТС должен начать тушение только в определённой точке, в определённом направлении и в течение определённого времени. При попытке осуществить пожаротушение в любой другой момент времени, в любом другом месте, или дольше положенного, модуль безопасности должен пресечь тушение.

Возможные инциденты:

4.1. Тушение не в точке пожара (уровень критичности: высокий)

4.2. Тушение не в направлении пожара (уровень критичности: средний)

4.3. Тушение дольше положенного (уровень критичности: низкий)

# 2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ

Задания состоят из модулей, выполняемых последовательно. Оценивание производится экспертами после сдачи конкурсантами решения всех модулей, согласно критериям оценки.

Конкурсное задание выполняется исключительно с использованием цифрового двойника АНТС и полигона в физическом симуляторе на основе «GAZEBO».

Необходимое программное обеспечение, подробные пояснения к заданию, примеры решений и документация находятся в репозиториях GitFlic по ссылке: https://gitflic.ru/company/agts-mre. Конкурсанты получают доступ к репозиториям в соревновательные дни.

## 2.1. Личный инструмент конкурсанта

Конкурсанту разрешается использовать собственные инструменты, указанные в инфраструктурном листе, а также следующие инструменты:

* клавиатуру на любом языке. Если конкурсант пользуется своей клавиатурой, и она выходит из строя, организатор предоставляет ему замену;
* языковые файлы для клавиатуры;
* мышь;
* USB-накопитель с музыкой;
* наушники проводные.

## 2.2. Материалы, оборудование и инструменты, запрещенные на площадке

Список материалов, оборудования и инструментов, которые запрещены на соревнованиях по различным причинам.

|  |  |  |
| --- | --- | --- |
| **Общие допуски и ограничения** | | |
| *Разрешенные действия* | *Запрещенные действия* | *Штраф* |
| Использовать встроенную справочную информацию используемых программ | Использовать запрещенные Интернет-ресурсы. Проносить на площадку «умные» часы и фитнес браслеты, микронаушники, заготовленные коды на любых носителях | За нарушение данного правила баллы, набранные конкурсантом за модуль, обнуляются |
| Самостоятельное выполнение конкурсного задания.  Поднятие сигнальных карточек для коммуникации с экспертами (см ТО) | Помощь третьих лиц, вербальное и невербальное общение во время модуля с целью получения преимуществ при выполнении конкурсного задания | В порядке, предусмотренном регламентом и правилами компетенции |
| Использовать инструкции от Команды по управлению соревнованиями | Самостоятельные действия без уведомления ГЭ, покидание рабочего (кроме случаев ЧП) | Штраф, согласно установленным правилам |
| Делать пометки в файлах КЗ, которые получают конкурсанты | Размещение на ноутбуке конкурсанта и использование в конкурсе домашних программ-заготовок, готовых кодов | Баллы, набранные участником, обнуляются |

## 2.3. Материалы, предоставляемые конкурсантам:

Всем предоставляется, в равных условиях:

1. Документация.
2. Программное обеспечение, эмулирующее автономное наземное транспортное средство (АНТС), которое проходит дистанцию в автономном режиме на основе маршрутного задания.

## 2.4. В ходе соревнований конкурсантам разрешается:

Модифицировать любым образом те фрагменты исходного кода АНТС, которые разрешены заданием. При этом ответственность за работоспособность изменений, или возможность/невозможность отменить неудачные изменения лежит полностью на конкурсанте.

## 2.5. В ходе соревнований конкурсантам запрещается:

* Менять любые элементы Симулятора АНТС, кроме фрагментов, явно указанных конкурсанту в задании и/или в интерфейсе пользователя Симулятора.
* Использовать в коде проверки, которые определяют наступление того или иного кибер-препятствия за счет знания исходного кода полетного контроллера, участка трассы или времени события, или иных, кроме модуля безопасности, частей системы.
* Отключать код, приводящий к возникновению кибер-препятствий.
* Использовать любые (программные, или ручные или любые иные) средства воздействия на АНТС во время прохождения трассы, кроме предоставленных Симулятором.

В случае нарушения любого из этих пунктов конкурсант может оштрафован.

# 3. ПРИЛОЖЕНИЯ

Приложение 1. Инструкция по заполнению матрицы конкурсного задания

Приложение 2 Матрица конкурсного задания

Приложение 3. Инструкция по охране труда

1. *Указывается суммарное время на выполнение всех модулей КЗ одним конкурсантом.* [↑](#footnote-ref-1)