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

ОПИСАНИЕ КОМПЕТЕНЦИИ

«Кибериммунная автономность»

2025 г.

**Наименование компетенции**: Кибериммунная автономность

**Описание компетенции**

Кибериммунная автономность – создание автономных устройств, конструктивно устойчивых к кибератакам, способных работать и противостоять злоумышленникам без участия человека.

Навыки достижения кибериммунной автономности (или конструктивной безопасности при разработке программного обеспечения / программно-аппаратных комплексов) востребованы среди инженеров, программистов и специалистов по безопасности программного обеспечения.

Совсем скоро автономная умная техника будет окружать нас повсюду. Важно, чтобы она была защищена от киберугроз.

Автономные устройства строятся с использованием сложных компонент от разных производителей (например, автопилота), гарантировать отсутствие уязвимостей в котором не представляется реальным, а значит, уязвимости рано или поздно будут найдены и устройство будет атаковано. Необходимо, чтобы специалисты, которые их создают, умели закладывать устойчивость к возможным кибератакам сразу в конструкцию, чтобы обнаружение и эксплуатация уязвимостей злоумышленниками не привели к нарушению целей безопасности.

Добиться кибериммунной автономности разработчики могут за счет:

* хорошо спроектированной архитектуры устройства и его программного обеспечения;
* качественного, но небольшого по объему, доверенного кода;
* простых аппаратных решений для контроля критических подсистем.

Кибериммунная автономность позволяет значительно повысить безопасность автономных устройств интернета вещей, умных городов и предприятий, ускорить процесс тестирования на безопасность и выпуска автономных устройств на рынок, удешевить поддержку безопасности большого парка устройств и систем.

**Нормативные правовые акты**

Поскольку Описание компетенции содержит лишь информацию, относящуюся к соответствующей компетенции, его необходимо использовать на основании следующих документов:

* ФГОС СПО:
  + 09.02.07 Информационные системы и программирование(Приказ Минобрнауки России от 09.12.2016 N 1547 (ред. от 03.07.2024)
  + 10.02.05 Обеспечение информационной безопасности автоматизированных систем (Приказ Минобрнауки России от 09.12.2016 N 1553 (ред. от 03.07.2024)
  + 15.02.10 Мехатроника и мобильная робототехника (Приказ Минобрнауки России от 09.12. 2016 г. № 1550)
* Профессиональный стандарт:
* 06.001 «Программист», утвержден приказом Министерством труда и социальной защиты РФ от 20 июля 2022 года № 424н, зарегистрирован Министерством юстиции РФ от 22 августа 2022 года №69720
  + 06.033 Специалист по защите информации в автоматизированных системах, утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н, зарегистрирован Министерством юстиции РФ от 14 октября 2022 №70543

Перечень профессиональных задач специалиста по компетенции **о**пределяется профессиональной областью специалиста и базируется на требованиях современного рынка труда к данному специалисту*.*

|  |  |
| --- | --- |
| **№ п/п** | **Виды деятельности/трудовые функции** |
| 1 | **Формулировка целей безопасности автономной системы**  (на основе анализа бизнес-сценариев использования и во взаимодействии с заказчиком требуется определить события, которые приводят к критически неприемлемым событиям безопасности) |
| 2 | **Определение / выделение критического функционала автономной системы**  (при заданной программно-аппаратной архитектуре автономной системы и целях безопасности необходимо, используя принципы минимизации доверенной кодовой базы, определить критический функционал, нарушение работы которого приводит к неприемлемым для заказчика системы ущербам, модифицируя, при необходимости, архитектуру автономной системы без изменения ее функционала) |
| 3 | **Внедрение/подключение встраиваемых систем безопасности** (выполнить сборку программной и/или аппаратной составляющих автономной системы с подключением модуля безопасности в соответствии с ключевыми принципами обеспечения изоляции и контроля) |
| 4 | **Настройка встраиваемых систем безопасности**  (для определенных целей безопасности и для заданной архитектуры с выделенным критическим функционалом, разработать политики безопасности автономной системы на языке(ах) программирования, используемых в модуле безопасности) |
| 5 | **Верификация работы встраиваемых систем безопасности** (создать и выполнить ручные и/или автоматические тесты для проверки функционирования автономной системы и выполнения целей безопасности в условиях компрометации подсистем) |