УДК 004.056.53

ЗАЩИТА ПОДВОДНОГО ГЛАЙДЕРА ОТ НЕСАНКЦИОНИРОВАННОГО ВСКРЫТИЯ С ПОМОЩЬЮ ФОТОДАТЧИКА

А.А. Быков
(федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО», г. Санкт-Петербург)

Научный руководитель – С.С. Беляев
(федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО», г. Санкт-Петербург)

В работе рассмотрен способ защиты информации подводного глайдера при его несанкционированном вскрытии. Регистрация вскрытия осуществляется фотодатчиком.

Введение.
Подводные глайдеры выполняют ряд важных задач по сбору информации о подводном мире. Глайдер – автономный подводный аппарат, который способен выполнять свою миссию на протяжении длительного времени. Он может находиться в различных водных районах земного шара без наблюдения человека. В целом организация сбора данных с помощью глайдера влечет серьезные расходы компании: изготовление или покупка глайдера и систем, обеспечивающих его работу, установка необходимых датчиков для сбора информации, написание программы-миссии для глайдера, его выгрузка в воду. Полученная в результате информация также представляет собой коммерческую ценность. Утечка этой информации может нанести ущерб компании-владельцу глайдера.

Основная часть.
Структурно глайдер представляет собой герметическую торпедообразную конструкцию. Существует два способа получить доступ к информации глайдера: программный и аппаратный. При этом глайдер должен быть защищен от несанкционированного доступа к хранящейся в нем информации. Программный способ защиты обеспечивается различными средствами, например формой разъема и протоколами общения устройства и компьютера. Такой способ защиты представляет собой достаточно серьезную проблему, не справившись с которой, злоумышленник может попытаться считать данные напрямую из модулей запоминающих устройств на борту глайдера. Для этого необходимо вскрыть герметично закрытый корпус и произвести демонтаж электронных компонентов. В таком случае интерес представляет построение системы защиты информации глайдера от утечки на аппаратном уровне. Разнообразие аппаратных способов защиты меньше, чем программных, и наиболее эффективный в конкретном случае – самоликвидация носителя информации при регистрации факта несанкционированного вскрытия корпуса глайдера. Основу системы защиты составляют подсистема регистрации проникновения внутрь корпуса, подсистема самоликвидации носителя информации и подсистема отключения защиты. Первые две подсистемы предотвращают утечку информации, вторая – не допускает уничтожение информации при вскрытии глайдера владельцем.

Выводы.
Рассмотренный способ защиты информации подводного глайдера в случае его вскрытия позволяет предотвратить несанкционированный доступ к собранной глайдером информации.

Быков А.А. (автор) Подпись

Беляев С.С. (научный руководитель) Подпись