29 августа

Заголовок

**В ГУАП разработали метод защиты беспилотников от кибератак**

Анонс

Ученые ГУАП разработали систему обеспечения безопасности беспилотного транспорта, использующую технологии блокчейн и криптографии.

Текст

Об исследовании *написали РИА новости в разделе "Наука" https://ria.ru/20240827/nauka-1968129012.html*

Разработка позволяет избежать атак на "мозг" беспилотников.

В основе беспилотных систем (автомобилей, поездов и летательных аппаратов) лежит нейронная сеть и наборы данных, на которых сеть постоянно обучается. Эти элементы необходимо защищать от атак, которые могут привести к изменению "поведения" транспортного средства и как следствие к авариям.

– *Во-первых, нужно защищаться от вредоносных наборов обучающих данных, которые по своей сути похожи на вредоносные программы (трояны, вирусы и т.д.). Во-вторых, необходимо защищать саму сеть, на которую может быть совершена атака. Поскольку заранее предсказать поведение атакующего очень сложно, нам нужно было создать такую систему, которая будет безопасно храниться и обучаться*, – пояснил заведующий кафедрой информационной безопасности ГУАП Сергей Беззатеев.

Для обеспечения безопасности самой нейронной сети и обучающих ее наборов данных исследователи ГУАП разработали протоколы, основанные на различных криптографических алгоритмах, что гарантирует надежный сбор, хранение и обработку данных. При создании протоколов была использована технология открытого и частного блокчейн, которая работает по принципу матрешки и позволяет хранить и передавать информацию в виде последовательности блоков, каждый из которых содержит ссылку на предыдущий, что обеспечивает защиту данных от изменения и фальсификации.

Ключевой особенностью и потенциальным преимуществом разработки специалисты называют применение различных алгоритмов электронно-цифровой подписи, которые нужны для того, чтобы избежать подмены нейронной сети в транспортном средстве. Например, для подтверждения того, что сеть предназначена именно для этого беспилотника, специалисты предлагают использовать атрибутивную подпись. Она содержит отличительные черты конкретного транспортного средства, поэтому ее подлинность легко проверить.

Безопасность, по словам исследователей, обеспечивают также эффективные схемы консенсуса, основанные на системе голосования, то есть, прежде чем запустить беспилотное устройство, большинство разработчиков должны поставить свою электронную подпись, подтверждающую работоспособность и исправность нейронной сети.

Полученные результаты могут быть применены в системах Internet of Things/IoT (глобальной сети, которая позволяет "умным" устройствам взаимодействовать друг с другом). Это позволит существенно повысить эффективность реагирования соответствующих служб на события в IoT, а также проверять достоверность информации, получаемой из этих систем.

На данном этапе перед исследователями стоит задача разработки более эффективного протокола верификации событий с использованием элементов инфраструктуры IoT с учетом меняющегося уровня доверия к каждому из участников и наблюдателей события, вовлеченных в протокол его фиксации и верификации.

Исследование проводилось в рамках программы "Приоритет 2030", участником которой является Санкт-Петербургский государственный университет аэрокосмического приборостроения.