ПРИМЕНЕНИЕ ИНТЕРНЕТ ВЕЩЕЙ В ВОЕННОМ ДЕЛЕ

Способ С.П., Ахапкина А.М., Можейко В.Д.

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Abstract: The article deals with the the use of the Internet of things in military affairs.

Быстрому распространению Интернета вещей (Internet of things, IoT) способствует развитие машинного интеллекта и сетевых коммуникаций, причем «вещи» приносят больше пользы, когда они активно обмениваются информацией друг с другом. Это касается и интеллектуальной техники на полях боевых сражений — Интернета боевых вещей (Internet of Battle Things, IoBT), а также Internet of Military Things (IoMT) — интернет военных вещей. Интернет военных вещей включает в себя широкий спектр устройств, которые обладают интеллектуальными возможностями физического распознавания, обучения и срабатывания через виртуальные или киберинтерфейсы, интегрированные в системы. Эти устройства включают в себя такие элементы, как датчики, транспортные средства, роботы, БПЛА , носимые человеком устройства, биометрию, боеприпасы, броню, оружие и другие интеллектуальные технологии.

Применение IoT в армии исторически является классической задачей Автоматизированных Систем Управления Войсками (АСУВ), таких как, например, Единая Система Управления Тактическим Звеном (ЕСУ ТЗ).

Задача ЕСУ ТЗ определяется по классической схеме: необходимо связать воедино большой набор децентрализованных автономных систем, обеспечить слаженность работы системы в целом, её безопасность и целостность, увязать воедино всех разработчиков различного вида оборудования и контроллеров, определить протоколы связи и обеспечить их сопряжение с единой децентрализованной системой, обеспечить прозрачный контроль выполнения команд и задач в рамках функционирования системы в боевом режиме.

В целом, все АСУВ движутся в сторону повышения автономности РСУ (распределенная система управления), повсеместно внедряются технологии автономных интеллектуальных исполнительных устройств и датчиков (IoT, IIoT), искусственного интеллекта и машинного обучения, технологии дополненной и виртуальной реальности (AR, VR), технологии анализа неструктурированных данных (Big Data), технологии надёжных распределённых архивов (BlockChain). Некоторые функции АСУВ выносятся в облачные сервисы, в том числе локальные частные облака, распределённые мобильные ЦОД, в которых они размещаются.

Современный российский комплект снаряжения «Ратник 3.0» представляет собой целую сеть IoBT устройств: контроллер экзоскелета, шлем дополненной реальности, средства связи с высокой криптостойкостью, средства позиционирования, набор медицинских IoT для контроля состояния военнослужащего — и это не считая интеллектуального оружия.

Концепция армии США Future Combat Systems (FCS) также полностью включает весь приведённый стек технологий. Американская компания Nutanix, создающая технологии гражданской виртуализации для ЦОД, создала для вооружённых сил США мобильный ЦОД для построения локальных частных облаков прямо на поле боя, тактический дата-центр, фактически десантируемый облачный ЦОД в рамках проекта Deployable Joint Command and Control System.

В военной технике отрабатываются передовые средства связи: например, уже сейчас проектируются и испытываются средства беспроводной связи 6-го поколения. Именно военные определяют будущее гражданских технологий, лишь на военные бюджеты можно отработать и отладить технологии до их коммерческого применения.

В Вооруженных силах уже давно эксплуатируются сложнейшие IoMT/ IoBT — не только с удалённым управлением средствами разминирования, наземным транспортом доставки боеприпасов, различными роботизированными комплексами, но и полностью автономные летающие дроны со сверх- и гиперзвуковыми скоростями, с оффлайн-средствами идентификации и распознавания цели, а также алгоритмами на базе ИИ для принятия решения о её поражении.

Главная проблема развития такой огромной системы — это ее серьезная уязвимость. Противник будет осуществлять физические атаки против IoBT, воздействовать на него направленной энергией, „глушить" каналы радиосвязи, разрушать волоконно-оптические кабели и уничтожать источники электроснабжения. Кроме того, он будет принимать меры, направленные на нарушение конфиденциальности, целостности и доступности информации IoBT путем электронной прослушки и внедрения вредоносных программ.

Вооруженные силы — сильнейший драйвер развития технологий Интернета вещей. И не забывайте, многие IoT могут по запросу мгновенно превратиться в IoBT.

Литература

1. G.I. Seffers. Defense Department Awakens to Internet of Things. AFCEA.org, 1 Jan. 2015

2. A. Kott, D.S. Alberts, C. Wang. Will Cybersecurity Dictate the Outcome of Future Wars? // IEEE Computer. — 2015. Vol. 48, № 12. — P. 98–101