ТЕХНИЧЕСКИЕ И ОБЩЕСТВЕННЫЕ ДИСЦИПЛИНЫ

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ УСТРОЙСТВ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ ПИЛОТАМИ ВОЕННОЙ АВИАЦИИ

Институт информационных технологий БГУИР,
г. Минск, Республика Беларусь

Алешко Н.С., Анкуда Д.И.

Савенко А.Г.- магистр технических наук, ассистент

На сегодняшний день инструменты дополненной реальности применяются для решения широкого спектра задач, от медицины до компьютерных игр. Однако стоит отметить, что история применения AR начинается в военной авиации.

Первым устройством, использовавшим технологии AR, стал ИЛС (индикатор на лобовом стекле, head-up display (HUD)) британского самолета de Havilland Mosquito. Разработанный в 1942 году, он был призван совместить информацию, поступающую с РЛС с установленным на самолете прицелом, для обеспечения пилота информацией во время выполнения задач ночного истребителя. Совмещение происходило с помощью небольшого дисплея, установленного на одной линии с прицелом пилота [1].

Рисунок 1 – Современный ИЛС, установленный на истребителе F/A-18

Современные ИЛС позволяют демонстрировать пилоту значительно большее количество информации, например, такие показатели, как угол атаки, навигационные отметки при взлете\посадке, силу тяги двигателя и вектор траектории, а в вариантах системы, используемых военными-расстояние до цели, статус вооружения, положение сенсоров наведения, скорость сближения с целью [2]. Пример такого индикатора приведен на рисунке 1. Также у современных ИЛС существует возможность выводить на экран изображение с внешних источников, таких как подвесные контейнеры целеуказания и навигации, а также внешние видеокамеры [2].

Следующим шагом в использовании дополненной реальности в военной авиации стало создание систем нашлемного целеуказания и индикации (НСЦИ, Helmet-mounted display, HMD). Концепция устройства заключалась в выведении дополнительной информации прямо на индикатор, находящийся в шлеме пилота. Первым устройством данного типа стал Super Cockpit, разработанный по заказу ВВС США в 1969 году [3]. Конструктивно оно представляло из себя шлем, в котором совмещались дополненная и виртуальная реальность (более подробная схема изображена на рисунке 2). Основной целью разработки являлось упрощение выполнения задач на малых высотах [3].

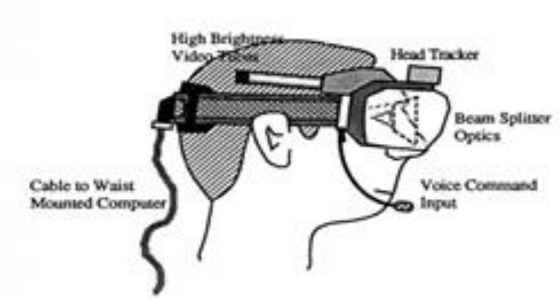

Рисунок 2 – Схема устройства Super Cockpit

В общем случае, нашлемная система целеуказания и индикации состоит из пяти основных частей: собственно, шлема, оптической системы, источника изображения, комплекса электронных систем, а также устройства отслеживания взгляда летчика. Сюда же могут входить и устройства, позволяющие ориентироваться ночью, например, модули ночного видения, которые крепятся к шлему пилота.

В дальнейшем системы HMD совершенствовались добавлением нового функционала, а именно выведения изображения с внешних камер и отображения информации о текущем состоянии летательного аппарата и маршруте полета (Integrated Helmet And Display Sight System (IHADSS), 1985 г. [4]). Очень важным событием стало создание НСЦИ «Щель-ЗУМ». Система позволяла осуществлять наведение ракеты «воздух-воздух» с помощью движений головы, что давало пилоту преимущество в воздушном бою [5]. «Щель-ЗУМ» являлась первой НСЦИ с таким функционалом, второй (и пока единственной, принятой в эксплуатацию) такой системой является Joint Helmet-Mounted Cueing System (JHMCS) (изображенная на рисунке 3), поставленной на вооружение ВВС США в 2003 году [6].

Рисунок 3 – Пилот в шлеме Joint Helmet-Mounted Cueing System

На сегодняшний день самой совершенной НСЦИ является Helmet-Mounted Display System (HMDS), разработанная специально для истребителя 5-го поколения F-35. В данном устройстве реализована интеграция с 6 внешними инфракрасными камерами, установленными на самолете, что позволяет пилоту осуществлять наблюдение буквально «вокруг» всего самолета. В шлеме присутствует возможность наведения всего спектра оружия, применяемого самолетом, а также возможность регулирования выводимой на дисплей НСЦИ информации. К примеру, пилот может выбрать отображаемые в визоре шлема параметры полета или цели [7]. Такой широкий спектр возможностей позволил конструкторам F-35 отказаться от ИЛС вовсе в пользу НСЦИ.

Проводя соответствующую оценку, можно выделить преимущества устройств дополненной реальности применительно к пилотам военной авиации.

Уменьшение времени реакции с помощью выведения и настройки объема необходимой информации с приборов на дисплей ИЛС\визор НСЦИ, что актуально при активном маневрировании, например, в ближнем воздушном бою. Особенно это касается НСЦИ с системой целеуказания – они позволяют использовать вооружение значительно быстрее, упрощая наведение до простого движения головы.

Стоит отметить и упрощение маневрирования летательного аппарата в целом. С помощью ИЛС\НСЦИ пилот может быть визуально проинформирован о том, какое маневрирование является безопасным, а какое – нет. Также стоит отметить возможность ИЛС\НСЦИ выводить пилоту информацию о рекомендуемых параметрах для взлета\посадки (которые считаются самыми опасными моментами в полете), включая скорость и высоту, а также систему «контрольных точек», что значительно упрощает действия пилота.

Однако у устройств дополненной реальности есть также очевидные недостатки.

Характерной особенностью некоторых НСЦИ является то, что конструктивно визор может использоваться лишь одним глазом, второй глаз при этом визором остается незадействованным. Из-за разницы в получаемом зрительной системой человека изображении пилоты могут ощущать дискомфорт, вплоть до сильной головной боли [8]. Также стоит отметить большую массу НСЦИ, что приводит к большой нагрузке на шею носителя и вызывает боли в спине [9].

Значимой проблемой является информационная перегрузка. Несмотря на то, что в современных НСЦИ и ИЛС существует возможность фильтрации выводимой информации, в некоторых ситуациях потоки данных, демонстрируемые пользователю, не могут быть своевременно им обработаны, что увеличивает вероятность совершения пилотом ошибки. Особенно это опасно при выполнении сложных маневров на малой высоте или во время нахождения в зоне боевых действий.

Еще одной общей проблемой устройств дополненной реальности в военной авиации является их сложность и, следовательно, надежность. Большая часть современных НСЦИ испытывает проблемы как на стадии разработки, так и на стадии непосредственной эксплуатации [10]. Эти проблемы являются решаемыми и своевременно исправляются, однако на время внесения исправлений в аппаратную или программную части НСЦИ перестает быть рабочим инструментом.

Сложность AR-устройств также потенциально уменьшает темпы подготовки пилотов. Учитывая все возможности НСЦИ, пилота требуется дополнительно обучать использовать функционал устройства, что занимает достаточно большой промежуток времени ввиду наличия широкого спектра инструментов.

Несмотря на все недостатки, устройства дополненной реальности находят все более широкое применение в военной авиации, что говорит о том, что риск их использования в сравнении с преимуществами все же не является настолько большим. С учетом постоянного совершенствования технологий и развития возможностей AR, вышеперечисленные проблемы могут быть решены в самом скором времени.

Список использованных источников:

1. White I. The History of Air Intercept (AI) Radar and the British Nightfighter /I.White.– Casemate Publishers, 2007..– 326 p.
2. Spitzer, Cary R., ed. Digital Avionics Handbook. Head-Up Displays. – Boca Raton, FL: CRC Press, 2001. – 206 p.
3. Military Applications of Augmented Reality / Mark A. Livingston [and other]. – Washington: Naval Research Laboratory, 2011. – 36 p.

4. USAARL Report No. 88-13 [Электронный ресурс]. – Режим доступа: http://www.usaarl.army.mil/TechReports/88-13.PDF. – Дата доступа:18.03.2018

5. Авиашлемы. Виртуальная реальность в настоящем бою [Электронный ресурс]. – Режим доступа: https://naked-science.ru/article/tech/aviashlemy-virtualnaya-realnost-v/. – Дата доступа: 18.03.2018.

6. Joint Helmet Mounted Cueing System [Электронный ресурс]. – Режим доступа: https://www.rockwellcollins.com/Products and Services/Defense/Avionics/Displays and Controls/Helmet Mounted Displays/ Joint Helme Mounted Cueing System.aspx. – Дата доступа: 18.03.2018

7. F-35 Gen III Helmet Mounted Display System [Электронный ресурс]. – Режим доступа: https://www.rockwellcollins.com/Products and Services/ Defense/Avionics/Displays and Controls/Helmet Mounted Displays/F-35 Gen III Helmet Mounted Display System.aspx. –Дата доступа: 18.03.2018

8. Rash C.E. Helmet Mounted Displays: Design Issues for Rotary-wing Aircraft / C. E. Rash. – SPIE, 2001. – 258 p.

9. Newman D.G. Flying Fast Jets: Human Factors and Performance Limitations/D.G. Newman.– CRC Press, 2014.– 184 p.

10. Pentagon: Here are all the problems with the F-35 [Электронный ресурс]. – Режим доступа: http://www.businessinsider.com/here-are-all-the-problems-with-the-f-35-that-the-pentagon-found-in-a-2014-report-2015-3. – Дата доступа: 18.03.2018.

УГРОЗЫ ДЛЯ УСТРОЙСТВ, РАБОТАЮЩИХ ПОД УПРАВЛЕНИЕМ ОС ANDROID

Институт информационных технологий БГУИР,
г. Минск, Республика Беларусь

Бакунович Д.В.

Пачинин В.И., зав. кафедрой ИСиТ, к.т.н.,доцент

В докладе проведен анализ угроз для устройств, работающих под управлением ОС Android. На основе проведенного анализа рассмотрен ряд примеров устранения возникающих угроз и расширения возможностей программных продуктов.

В настоящее время мобильные устройства активно внедряются во все сферы жизни современного человека. Смартфоны, планшеты, электронные книги – все эти устройства уже стали неотъемлемой частью жизни. Большинство мобильных устройств работают на ОС Android. Однако эта ОС используется практически везде: начиная от домашних бытовых приборов (холодильники, телевизоры и т.д) и заканчивая различными помощниками управляемых голосом, жестами и т.д. Существуют системы “Умный дом” которые управляются при помощи голоса, жестов и приложений.

Такое широкое распространение ОС Android повлияло на очень быстрый рост различных вредоносных программ. Сначала они были весьма безобидными: показывали рекламу, воровали деньги путем рассылок платных смс, блокировали работу устройства (баннеры-вымогатели), но из-за стремительного роста Android, вредоносные программы становились все более изощренными и опасными. К примеру, развитие интеллектуальных помощников, которые могут совершать покупки в интернет магазинах, при помощи вредоносной программы можно похитить денежные средства, делать фото, включать микрофон, а также повлиять на работу всех функций, которые может использовать система. Например, была ситуация, когда система “умный дом” была заряжена трояном-вымогателем. Уязвимость в приложении “умного” термостата позволяла дистанционно поднимать или опускать температуру, а после этого требовала выкуп за возвращение контроля. Данная уязвимость, в случае отсутствия хозяев либо их сна, может привести к таким негативным последствиям, как различные болезни от переохлаждения или даже смерти домашних животных.

Для удаленного управления различными устройствами используются приложения на смартфоне. Чаще всего в таких приложениях отношение к безопасности посредственное и наиболее распространенными уязвимостями являются:

— Нет проверки целостности кода. Данная уязвимость позволяет добавлять свой вредоносный код или целиком менять различные функции в приложении.

— Нет обфускации. Это значит, что при декомпиляции приложения код никак не защищен и злоумышленник может просмотреть как реализовываются те или иные функции, что позволит потенциально добраться до дыр в системе.

— Нет технологии обнаружения root. Права суперпользователя позволят вредоносным программам полностью взять контроль над устройством.

— Нет зашифрованные логин и пароль. Доступ к внутренним файлам приложения позволит получить персональные данные пользователей.

— Нет защиты от троянов, которые помещают свое окно поверх окна приложения. Распространенная уязвимость, которая позволяет обманом вынудить ввести логин и пароль через фишинговое окно.

Например, автомобиль Tesla уже неоднократно дистанционно взламывался с практически полным контролем над мультимедийной системой автомобиля. Но такие взломы обычно строятся на основе компрометации бортового ПО самого автомобиля. Но специалисты решили атаковать официальное Android-приложение Tesla. Пользователь, после установки приложения, должен ввести имя пользователя и пароль, после которого формируется токен OAuth. Исследователи выявили, что токен хранится в незашифрованном виде в директории sandbox. Получив токен уже доступен ряд некоторых действий над автомобилем, однако одного токена недостаточно для запуска двигателя. Для того, чтобы получить полный доступ к автомобилю можно установить вирус с root доступом, который скопирует данные на необходимый адрес. Специалисты пошли