004.522:004.056.5

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ГОЛОСОВЫХ АССИСТЕНТОВ

Бурым Н.С., Балакшин П.В.
(Университет ИТМО)
Научный руководитель – к.т.н. Балакшин П.В.
(Университет ИТМО)

В данной работе уделяется внимание рискам нарушения конфиденциальности при использовании голосовых ассистентов.

Введение. В области информационных технологий средства взаимодействия пользователя с технической системой называют интерфейсом. Интерфейсы бывают разные и реализуются разными средствами и методами. Одной из важнейших задач разработки современных технических систем является обеспечение наиболее интуитивного и естественного интерфейса с пользователем.

Одной из естественных форм взаимодействия для человека является речь. Голосовой интерфейс является одним из ключевых частей человеко-машинного взаимодействия, позволяющий улучшить существующий пользовательский интерфейс, а также обеспечить более удобный способ взаимодействия человека с компьютером. Голосовой поиск от компании Google и голосовой ассистент Siri от компании Apple являются основными примерами, подтверждая насущную необходимость внедрения речевых технологий, в частности распознавания речи и голосовых интерфейсов.

Подключенные к Интернету гаджеты с голосовыми помощниками, становятся все более популярными благодаря их удобству для повседневных задач, таких как вопросы о прогнозе погоды, воспроизведение музыки или управление другими умными вещами в доме. Однако такое удобство сопряжено с риском для конфиденциальности. Например, интеллектуальные гаджеты должны постоянно слушать окружающую среду, чтобы активироваться, когда произносится «пробуждающее слово», и, как известно, они передают звук из своей среды и записывают его на облачные серверы.

Цель работы. Целью работы является исследование современных проблем в области безопасности современных голосовых ассистентов.

Выводы. Быстрое внедрение постоянно включенных умных голосовых помощников у себя дома, на предприятиях и в общественных местах вызвало ряд опасений со стороны защитников конфиденциальности. Хотя эти устройства предлагают удобное голосовое взаимодействие, их микрофоны всегда слушают слова пробуждения. По мере того, как умные колонки становятся все более распространенными в повседневной жизни, возникает острая необходимость в понимании поведения этой экосистемы и ее воздействия на потребителей. В этой работе мы рассмотрели несколько уязвимостей безопасности умных колонок и голосовых ассистентов. Главным недостатком современных голосовых помощников является то, что без контроля доступа на основе физического присутствия они могут принимать голосовые команды, даже когда поблизости нет людей.

Бурым Н.С. (автор)

Балакшин П.В. (автор, научный руководитель)