

с тем, определение слуховой чувствительности является весьма трудоемким процессом. На результаты измерений могут оказывать ряд факторов, исключить влияние которых является весьма проблематичной задачей. Первое с чем сталкивается исследователь это весьма высокие внешние акустические шумы. Для исключения этого фактора определение порога восприятия чистых тонов необходимо проводить в акустически заглушенной камере с уровнем звукового давления фонового акустического шума в диапазоне частот 100 Гц – 10000 Гц не более 20 дБ.

Второе, это методика формирования тестовых сигналов. Наиболее удобный вариант это формирование тестовых сигналов с помощью компьютера и воспроизведение тоновых акустических сигналов с заданным уровнем звукового давления и контроль уровня звукового давления в месте расположения аудитора. Тестовый сигнал необходимо формировать на частотах 500, 1000 и 2000 Гц с повышением уровня звукового давления от 0 дБ до 10 дБ с шагом 0,25 дБ. При этом время воспроизведения акустического сигнала на каждой ступени должно составлять от 3 до 5 с. Переход от одного уровня сигнала к другому уровню сигнала необходимо выполнять при переходе синусоидального сигнала через ноль. Кроме тестового сигнала с повышением уровня звукового давления необходимо формировать тестовый сигнал, с понижением уровня звукового давления начиная с 10 дБ до 0 дБ с шагом 0,25 дБ. Изменение уровня сигнала также выполняется при переходе синусоидального сигнала через ноль. При экспериментальных исследованиях у аудитора должны быть кнопка для подтверждения слухового восприятия акустического сигнала.

Третье, измерение уровня звукового давления в месте расположения аудитора необходимо выполнять с использованием высокочувствительного микрофона с предварительным усилителем с уровнем собственных шумов не более 0 дБ в диапазоне частот от 10 до 10000 Гц. Такими характеристиками обладает микрофонный капсюль 4179 с предварительным усилителем 2660 фирмы «Bruel & Sound & Vibration Measurement A/S». Сигнал, принятый от микрофона необходимо пропустить через узкополосный полосовой фильтр для выделения чистых тонов, на которых проверяется порог восприятия.

Слуховая чувствительность аудиторов в сильной степени зависит от состояния аудитора. Если в течении последних суток перед измерением слуховой чувствительности аудитора он находился в условиях воздействия акустических шумов с уровнем звукового давления порядка 100 дБ в течении получаса или на его слуховой аппарат от наушников воздействовали повышенные уровни звукового давления, результаты проверки слуховой чувствительности дадут заниженные показатели. Это подтверждает тот факт, что слуховая чувствительность аудитора изменяется от состояния аудитора. Поэтому при оценке разборчивости маскируемой шумами речи кроме отбора аудиторов необходимо проводить их обучение и подготовку к проведению работ по распознаванию речи [1].

Работа выполнена при поддержке грантового финансирования КН МОН РК, № AP05130293.

Список литературы

1. Method for protecting speech information / H.V. Davydau [et al.] // Doklady BGUIR. 2015. № 8 (94). P. 107–110.

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ РОЕВЫХ РОБОТОВ

А.В. Сидоренко, М.С. Шишко

Безопасность в информационной среде, включая роботизированные роевые системы, принципиально связана с предоставлением основных услуг, таких как конфиденциальность данных, целостность данных, аутентификация объектов и аутентификация источника данных.

В отличие от других областей, в которых активно проводятся исследования, связанные с безопасностью, роботизированные роевые системы испытывают недостаток практических решений этих проблем [1]. Тема безопасности была упущена из современных исследований в основном из-за сложных и гетерогенных характеристик роботизированных систем: автономии роботов, децентрализованного контроля, потенциально большого количества членов роя, коллективного поведения и т. д.

Технология блокчейн может обеспечить не только надежный peer-to-peer канал связи для агентов роя, но также способ преодоления потенциальных угроз, уязвимостей и атак [2]. Блокчейн – это новая технология, возникшая в поле биткоин, и демонстрирующая, что с помощью объединения одноранговой сети с криптографическими алгоритмами, группа агентов может достичь соглашения по конкретному положению дел и зафиксировать это соглашение без необходимости обращения к контролирующему органу. Комбинация блокчейна с другими распределенными системами, такими как роботизированные роевые системы, может предоставить необходимые возможности, для того, чтобы сделать операции внутри роботизированного роя более безопасными, автономными и гибкими.

Наличие распределенных данных может облегчить реализацию некоторых алгоритмов роевой робототехники и может проложить путь для новых приложений роевой робототехники (например, алгоритмам машинного обучения). Использование технологии блокчейна в качестве децентрализованной защищенной системы управления может быть полезным при решении широкого спектра задач. Распределенная система хранения данных внутри роя накладывает дополнительные требования к вычислительным ресурсам и памяти отдельных участников роя. Следовательно, данный подход может использоваться для отдельных задач и систем в робототехнике.

Список литературы

1. Higgins F., Tomlinson A., Martin M. Security Challenges for Swarm Robotics // Technical Report. University of London, Royal Holloway, Department of Mathematics, October 2008.
2. Strobel V., Dorigo M. Blockchain technology for robot swarms: A shared knowledge and reputation management system for collective estimation // Technical Report Series. IRIDIA, 2018.

ПРОБЛЕМЫ ВЫСШЕЙ ШКОЛЫ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.Б. Соколов

Одной из основных проблем высшей школы при подготовке специалистов в области информационной защиты является недостаточная квалификация преподавательского состава. В основном такое положение вещей связано с практической невозможностью переподготовки преподавателей высшей школы в условиях, изменяющихся столь стремительно. Расширение информационного поля, появление новых способов защиты информации, новых информационных потоков – все это предполагает мобильность учебного процесса, его постоянное изменение и совершенствование. Но для подобных изменений, для организации мобильного учебного процесса, соответствующего реальной действительности в каждый момент времени, нет ни материально-технической, ни даже мотивационной базы, и переподготовка специалистов-преподавателей не осуществляется. Оснащенность лабораторий для занятий такова, что по большей части ознакомление студентов с современными техническими средствами защиты информации можно осуществлять лишь в теории, не переходят к практике.

Российские специалисты в области информационной защиты обращают особое внимание на недостаточность учебников – учебные пособия также отстают от действительности. Они предлагают решать данный вопрос на государственном уровне, создавая на государственные деньги в университетах творческие коллективы, которые могли бы заниматься разработкой новых учебников.

Кроме того, практически нет связи между высшей школой и потенциальными работодателями будущих специалистов в области информационной защиты, а именно такая связь может обеспечить необходимую мобильность учебного процесса и стимулирование инновационного мышления как преподавателей, так и студентов. Но в настоящее время положение вещей таково, что преподаватели неуклонно отстают от изменяющихся условий, соответственно, при этом падает уровень преподавания и подготовки специалистов.