4. Об утверждении Государственной программы развития цифровой экономики и информационного общества на 2016-2020 годы / Постановление Совета Министров Республики Беларусь от 23 марта 2016 г. № 235. URL: http://etalonline.by/document/?regnum=c21600235&q_id=754193 (дата обращения 02. 05.2019).

МЕХАТРОННАЯ СИСТЕМА ПАРАЛЛЕЛЬНОЙ КИНЕМАТИКИ

В.В. Кузнецов

Для технических средств защиты информации основанных на мехатронных системах остро ставится задача повышения точности и быстродействия исполнительных механизмов и используемых мехатронных систем перемещений. Эффективным средством решения этой задачи является широкое использование мехатронных систем параллельной кинематики с многокоординатным приводом прямого действия. Для таких систем нами была предложена концепция управляемого движения в трехмерном пространстве на базе многокоординатного привода и реконфигурируемых механизмов параллельной кинематики [1].

В настоящей работе в развитие этой концепции представлены новые результаты по разработке систем многокоординатных перемещений, математических моделей и алгоритмов для их компьютерного имитационного моделирования. Предложена новая мехатронная система перемещений с шестью степенями свободы, построенная на гибридном приводе прямого действия, компонуемого из трех линейных и трех поворотных программно-управляемых координатных позиционеров кинематически связанных с исполнительным механизмом параллельной кинематики в виде раскрывающегося тетраэдра.

Такая компоновка мехатронной системы позволяется реализовывать прецизионные движения с шестью степенями свободы по шести независимым координатам в трехмерном пространстве, включая три линейных и три угловых, обеспечивая повышенные кинематические и динамические характеристики перемещений при высокой точности их реализации.

Список литературы

1. Системы многокоординатных перемещений на механизмах параллельной кинематики / С.Е. Карпович [и др.]. Минск : Бестпринт, 2017. 254 с.

РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УСТРОЙСТВ НОСИМОЙ ЭЛЕКТРОНИКИ

В.Ф. Кулиш

Согласно прогнозам компании Gartner в 2022 г. будет продано 453,19 миллион единиц устройств носимой электроники. Наиболее распространенными устройствами такого типа являются фитнес-браслеты. Они позволяют собирать данные о физической активности пользователей (количество пройденных шагов, пройденная дистанция, сожженные калории, данные о занятиях спортом и сне, данные о пульсе). Собранная информация отправляется на удаленный сервер для дальнейшей обработки. Браслет представляет собой, как правило, следующий набор датчиков (акселерометр, оптический датчик измерения пульса), а также микропроцессоры, необходимые для обработки информации от датчиков и передачи этих данных на смартфон с помощью технологии Bluetooth. Архитектура для обработки данных состоит из следующих компонентов: браслет для сбора информации, смартфон для получения информации с браслета, отправки данных на сервер и получение обработанных результатов, сервер для обработки полученных данных. Основными рисками информационной безопасности такой системы является утечка данных о пользователе, а также подмена отправляемой информации. Риск утечки информации может быть реализован с помощью следующих атак:

– перехват коммуникаций между браслетом и смартофоном;

– обход механизма аутентификации в браслете;

– создание фантомного устройства для получения статистических данных с удаленного сервера.

Риск отправки поддельных данных может быть реализован с помощью атак на сетевой приложение на сервере, а также с помощью манипуляции данных передаваемых мобильному приложению для последующей отправки.

АУДИТ БЕЗОПАСНОСТИ ТРАФИКА В СИСТЕМЕ IP-ТЕЛЕФОНИИ

Д.В. Куприянова, Д.Н. Одинец

Протоколы SIP и RTP, используемы для передачи медиа данных, были разработаны без учета необходимости защищать передаваемую информацию, в следствии чего возможны следующие виды атак и уязвимостей: фрод звонков, вирус, попавший в сеть IP-телефонии может начать рассылать спам ее абонентам, нарушение звонков – атакующий рассылает пакеты клиентам звонка, DoS – за счет отправки большого количества сообщений «Invite» и «Registrer» нарушается работу компонентов SIP, атакующий прослушивает весь трафик в IP-телефонии, подбор паролей, Man-In-The-Middle – атакующий проникает в звонок между пользователями, и может не только прослушивать, но и изменять сообщения между клиентами.

Для защиты передаваемы данных, предлагается использовать протокол TLS – протокол защиты транспортного уровня. Данный протокол использует асимметричное шифрования для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений. Также для защиты данных может быть использован IPsec – набор протоколов для обеспечения защиты данных, передаваемых по протоколу IP, обеспечивающих аутентификацию, проверку целостности и/или шифрование IP-пакетов. В отличие от IPSec, TLS протокол реализуется на транспортном уровне и не требует поддержки на промежуточных устройствах.

Для улучшения защиты может быть использован VPN. В случае невозможности использования VPN, необходимо использовать VLAN. Данные решения создают виртуальную сеть, что позволяет передавать данные в надежных сетях.

В данном случае лучшим выбором будет использование VPN который позволяет шифровать данные, так как в этом случае нет необходимости реализации шифрования на клиентах, отсутствует риск ошибок в реализации шифрования, VPN может быть обновлен для использования более современных методов шифрования без необходимости обновления кода клиента [1–3].

Список литературы

1. Security in a SIP network: Identifying network attacks [Электронный ресурс]. URL: https://searchunifiedcommunications.techtarget.com/feature/Security-in-a-SIP-network-Identifying-network-attacks (дата обращения: 05.04.2019).

2. How to Address WoIP Security Challenges [Электронный ресурс]. URL: http://www.centurylinkbrightideas.com/how-to-address-voip-security-challenges/ (дата обращения: 05.04.2019).

3. SIP Server Security with TLS: RPE [Электронный ресурс]. URL: https://www.researchgate.net/publication/235601569_SIP_Server_Security_with_TLS_Relative_Performance_Evaluation (дата обращения: 05.04.2019).

СПОСОБЫ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Д.В. Куприянова, Д.Ю. Перцев

Анализ ситуации, проведенный BSA Global Software Survey [1], показывает, что рынок нелицензионного ПО уменьшается, однако по состоянию на 2018 г. составляет 37 % и оценивается более чем в 46 млрд. долларов. С учетом этого проблема защиты авторских прав по-прежнему является актуальной. К основным способам защиты ПО относится: лицензионный ключ, жесткая привязка к носителю информации, USB-ключ. Лицензионный ключ является самым простым способом защиты и предполагает генерацию ключа по некоторому шаблону с привязкой к имени пользователя или аппаратной конфигурации системы. Основным