Что касается белорусских производителей, то, так как деанонимизация пользовательской статистики не является требованием белорусского законодательства, то и алгоритмы дифференциальной приватности и аналогичные средства ими не применяются.

Список литературы

1. Narayanan, A., Shmatikov V. Robust De-anonymization of Large Sparse Datasets // 2008 IEEE Symposium on Security and Privacy (sp 2008). URL: https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (дата обращения: 03.05.2019).

ПРЕПОДАВАНИЕ ДИСЦИПЛИН В ОБЛАСТИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ СПЕЦИАЛЬНОСТЕЙ ПЕРВОЙ И ВТОРОЙ СТУПЕНЕЙ ВЫСШЕГО ОБРАЗОВАНИЯ

Е.А. Криштопова, В.С. Осипович, А.М. Прудник

В настоящее время, вопросам информационной безопасности в Республике Беларусь придается очень большое значение [1, 2], кроме того, одним из государственных приоритетов нашей страны провозглашена ориентация на информационное общество и развитие рынка инфокоммуникационных технологий [3, 4].

Исходя из этого, для высших учебных заведений одной из актуальных проблем является подготовка специалистов как в области безопасности информационных технологий, так и в смежных областях с соответствующими компетенциями.

В свете стоящих задач, на кафедре инженерной психологии и эргономики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» начато преподавание ряда дисциплин в области безопасности информационных технологий.

На 1-й ступени высшего образования по специальности 1-58 01 01 «Инженерно-психологическое обеспечение информационных технологий» преподается дисциплина «Криптографические технологии», в рамках которой изучаются базовые принципы криптографии, современные криптографические протоколы, студенты овладевают навыками применения криптографических технологий для защиты информации. На данную дисциплину для студентов дневной формы обучения отводится 32 академических часа лекций и 32 академических часа практических занятий.

Для студентов 2-й ступени высшего образования по специальности 1-59 81 01 «Управление безопасностью производственных процессов» преподается дисциплина «Безопасность информационных систем». Целью изучения дисциплины является получение знаний по вопросам обеспечения безопасности информационных систем в условиях различных по виду, происхождению и характеру возникновения угроз. На данную дисциплину для студентов дневной формы обучения отводится 10 академических часов лекций и 20 академических часов практических занятий.

Таким образом, внедрение кафедрой инженерной психологии и эргономики актуальных учебных дисциплин в области безопасности информационных технологий способствует решению задач качественной подготовки инженерных кадров в соответствии с вызовами времени.

Список литературы

1. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации». URL:http://etalonline.by/document/?regnum=h10800455&q_id=754382 (дата обращения 02. 05.2019).

2. Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь». URL:http://etalonline.by/document/?regnum=p219s0001&q_id=754197 (дата обращения 02. 05.2019).

3. Стратегия развития информатизации в Республике Беларусь на 2016–2022 годы / Постановление коллегии Министерства связи и информатизации Республики Беларусь от 30.09.2015 г. № 35. URL: http://etalonline.by/document/?regnum=u215e2913&q_id=754159 (дата обращения 02. 05.2019).

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.