



Кафедра компьютерных систем и сетей



Научно-технический центр  
Гарантоспособные (надежные и безопасные)  
системы, сервисы и технологии



Научно-технический семинар  
**Критические компьютерные технологии и системы**  
(КриКТехС-2017/5/122)

## ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

На кафедре компьютерных систем и сетей с 31 мая 2001 года работает постоянно действующий Всеукраинский научно-технический семинар КриКТехС «Критические компьютерные технологии и системы» [crictecs.csn.khai.edu](http://crictecs.csn.khai.edu)

Основные направления работы семинара связаны с анализом, моделированием, разработкой, экспертизой и применением компьютерных (программных, программируемых и аппаратных) средств, систем, сетей и ИТ-инфраструктур для критических и коммерческих приложений с учетом требований к надежности, живучести, функциональной и информационной безопасности.

Научный руководитель семинара – заслуженный изобретатель Украины, доктор технических наук, профессор заведующий кафедрой компьютерных систем и сетей (№503) Харченко Вячеслав Сергеевич.

Информационный администратор – старший преподаватель кафедры №503 Перепелицын Артём Евгеньевич.

тел. 057-788-45-03, 057-788-43-56,

e-mail: [y.kharchenko@csn.khai.edu](mailto:y.kharchenko@csn.khai.edu), [a.perepelitsyn@csn.khai.edu](mailto:a.perepelitsyn@csn.khai.edu)

адрес: Украина, 61070, Харьков, ул. Чкалова, 17, ХАИ, кафедра №503

Очередное заседание семинара состоится 30 июня (пятница) 2017 г., в 15:00 в аудитории 238 радиокорпуса ХАИ.

Тема заседания: Методы малоресурсной и постквантовой криптографии и перспективы их применения в промышленных системах

Доклады:

1. Чевардин Владислав Евгеньевич (кандидат технических наук, с.н.с., доцент кафедры информационной безопасности и киберзащиты, Военный институт телекоммуникаций и информатизации, Киев). Псевдослучайные бит-генераторы и методы малоресурсной криптографии в контексте развития квантового компьютеринга:

- анализ возможностей будущих квантовых компьютеров;
- псевдослучайные бит-генераторы, основанные на эллиптических кривых (ЭК)
- новые методы построения;
- перспективы малоресурсной криптографии на основе ЭК.

2. Федосеева Алина Александровна (ассистент кафедры фармакоинформатики, Национальный фармацевтический университет, Харьков). Модели, методы и инструментальные средства оценивания качества безопасности ПО АСУТП лекарственных препаратов (ЛП):

- актуальность обеспечения качества и безопасности ПО АСУТПЛП;
- анализ стандартов и разработка нормативного профиля ПО таких систем;
- модели процессов и методы оценки качества и безопасности ПО;
- инструментальное средство «AFEUR»: общая характеристика и применение.

3. Вамболь Алексей Сергеевич (аспирант кафедры компьютерных систем и сетей, ХАИ). Постквантовая криптография и перспективы ее применения для Интернета вещей (IoT):

- краткий обзор методов постквантовой криптографии;
- перспективы и особенности применения методов постквантовой криптографии в IoT системах;
- структура модуля «Введение в постквантовую криптографию», проект SEREIN.

Информация о проектах, конференциях, семинарах:

Харченко Вячеслав Сергеевич (доктор технических наук, профессор, кафедра компьютерных систем и сетей ХАИ):

- о Global Cybersecurity Summit, Киев, 14-15 июня 2017 <https://gcs17.com/ua/>
- об участии в летней школе по проекту PERCCOM (ERASMUS+): подготовка магистров в области Pervasive Computing and Communications for Sustainable Development, Великобритания, Лидс, 19-23 июня 2017 <http://perccom.univ-lorraine.fr/>
- о подготовке издания 3 тома Green IT Engineering: Social, Business and Industrial Applications", Volume 3, серия "Studies in Systems, Decision and Control", Springer <http://www.springer.com/series/13304>