Јавно предавање

НЕКИ ОТВОРЕНИ ПРОБЛЕМИ И НАПРЕЦИ

У ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ И БЛОКЧЕЈН ТЕХНОЛОГИЈИ

Дописни члан САНУ Миодраг Михаљевић

Четвртак, 24. новембар, 12 сати

Мултимедијална сала Универзитета у Нишу

***Сажетак***

Информационо-комуникационе технологије (ИКТ) и дигитални (сајбер) простор су нераскидиво повезани са нашим физичким тродимензионалним простором. Они се стално проширују и пружају нам нове погодности.

Блокчејн технологија и информациона безбедност су изузетно битне компоненте и за ИКТ и у дигиталном простору као подршка изузетно великом броју активности. Механизми информационе безбедности треба да омогуће да све добробити које нам пружа дигитални простор не постану отворена врата за злонамерне активности са потенцијално катастрофалним последицама. Стога је информациона безбедност прва линија заштите наше приватности у сајбер простору.

Блокчејн технологију је прославила њена прва широко распрострањена примена, крипто валута Биткоин, али је ова технологија неупоредиво већег значаја од њене прве општепознате примене. Она је отворила могућности нових парадигми у дигиталном простору, укључујући дистрибуирану верификацију без овлашћеног верификатора и такозване паметне уговоре, који отварају нове могућности у дигиталној економији.

Сајбер простор се свакодневно увећава и преплиће са нашим реалним тродимензионалним простором, стварајући оно што се данас назива Метаверзумом – у овом контексту изузетно се увећавају и значај и садржаји информационе безбедности и блокчејн технологије.

Циљ излагања је да експертски али и примерено широј јавности укаже на илустративне напретке у техникама за информациону безбедност и блокчејн технологију. У предавању се истиче да је један од кључних изазова у техникама истовремено обезбеђивање високе сигурности и малог додатног надоптерећења. Као илустрација напредака у домену информационе безбедности указује се на један приступ ојачавању криптографске сигурности алгоритама шифровања ниске имплементационе сложености применом резултата теорије информација и кодова.

Напреци у техникама за болкчејн технологију илуструју се приказом једног консензус протокола са суштински редукованом енергетском потрошњом и једног приступа за алијансно рударење резистентног на одређене злоупотребе.