ТЕМАТСКЕ ЦЕЛИНЕ САЈБЕР ПРАВА

I Основи сајбер безбедности и дигиталног правног оквира

1. Увод у сајбер безбедност
2. Европски правни оквир у области сајбер безбедности (НИС2, ДОРА, еИДАС2)
3. Закон о информационој безбедности Републике Србије
4. Стратегија развоја информационе безбедности и институционална архитектура
5. УН норме о одговорном понашању држава у сајбер простору и међународноправна одговорност државе за сајбер нападе (приписивост, дужност спречавања, противмере)

II ИКТ системи од посебног значаја – правни, организациони и технички аспекти

1. ИКТ системи од посебног значаја (приоритетни и важни ИКТ системи)
2. Самостални оператори ИКТ система од посебног значаја
3. Евиденција и обавезе оператора ИКТ система
4. Мере заштите ИКТ система од посебног значаја
5. Акт о процени ризика и Акт о безбедности
6. Обавештавање о инцидентима и поступање по пријему обавештења
7. Координисано откривање рањивости
8. Инспекција за информациону безбедност
9. База података о регистрацији домена

III Национална институционална структура сајбер безбедности

1. Надлежни органи за сајбер безбедност
2. Тело за координацију информационе безбедности
3. Национални ЦЕРТ – Канцеларија за информациону безбедност

4. ЦЕРТ органи власти

5. Посебни секторски ЦЕРТ-ови

6. Међународне организације и сарадња (ЕНИСА, ФИРСТ, ИТУ, ОЕЦД)

IV Високотехнолошки криминал – правни оквир, пракса и међународни стандарди

1. Увод у сајбер криминал – појам и појавни облици

2. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала

3. Правна и институционална инфраструктура борбе против ВТК у Републици Србији

4. Национални програм и стратешки оквир борбе против ВТК

5. Будимпештанска конвенција о сајбер криминалу

6. Други додатни протокол – међународна размена електронских доказа

7. Ханој конвенција Уједињених нација и друге конвенције од значаја.

8. Дигитални докази: прибављање, очување, међународна сарадња

9. Анонимност на интернету и проблеми идентификације учинилаца кривичних дела (посебне доказне радње у сајбер простору – тајни надзор, пресретање комуникација, нове истражне технике за деанонимизацију корисника)

V Вештачка интелигенција, манипулативне технологије и правни изазови

1. Злоупотреба вештачке интелигенције у сајбер криминалу (деепфаке, АИ-пхисхинг, аутоматизовани напади)

2. Европски АИ Акт – обавезе, ризици и правни стандарди

3. Стратегија развоја вештачке интелигенције Републике Србије и најављени АИ закон

4. Правни изазови модела великих језичких модела (ЛЛМ), аутономних система и алгоритамске одговорности

5. Доказне тешкоће код АИ генерисаних садржаја

VI ОСИНТ, дигитална форензика и прикупљање података

1. ОСИНТ технике – алати, методологија и правна ограничења

2. Правила и етички оквир за коришћење ОСИНТ техника у поступцима

3. Дигитална форензика и анализа инцидената

4. Идентификација преварних образаца, праћење извора и анализа ризика

VII Заштита деце на интернету

1. Национални и међународни правни оквир заштите деце у дигиталном окружењу

2. Савремени облици онлајн сексуалне експлоатације деце

3. Обавезе провајдера и државних органа

4. Превентивни и едукативни механизми

VIII Сајбер дипломатија и међународно решавање спорова

1. Сајбер дипломатија и међународни преговарачки процеси

2. Арбитража у сајбер и технолошким споровима

3. Мултилатерални формати и међународне иницијативе у домену дигиталне безбедности

4. Сајбер напади у контексту међународних оружаних сукоба и хибридног ратовања (сајбер напад као „оружани напад“ у контексту међународног права, услови за заснивање међународноправне одговорности државе за сајбер напад, примена међународног хуманитарног права у сајбер сукобима, међународна кривична дела извршена посредством сајбер средстава)