Табела 5.2. Спецификација предмета

Спецификацију треба дати за сваки предмет из студијског програма.

Студијски програм : Докторске студије

Назив предмета: Дигитална безбедност – сајбер простор и вештачка интелигенција

Наставник/наставници: проф. др Ненад Путник, проф. др Ана Ковачевић, проф. др Младен Милошевић

Статус предмета: обавезни

Број ЕСПБ: 8

Услов: нема

Циљ предмета

Студенти треба да усвоје нова и прошире постојећа знања о појму, садржају и значају дигиталне безбедности и вештачкој интелигенцији. Студенти ће се упознати са појмовима информационе и сајбер безбедности, сајбер ризика и претњи, и критичне информационе инфраструктуре. Разумеће методолошке проблеме везане за класификацију сајбер претњи и њихово место у различитим безбедносним парадигмама. Усвојиће знања о специфичним обележјима друштвених сукоба у дигиталном добу, као и о широком спектру њиховог испољавања. Упознаће се са појмом високотехнолошког криминала, његовом феноменологијом, узроцима, врстама и начинима извршења, као и националним и међународним правним оквиром за супротстављање. Стећи ће знања о стратешком оквиру сајбер безбедности и новом концепту сајбер суверенитета, као и о активностима националних армија у сајбер простору, те глобалним иницијативама за постизање сајбер мира. Упознаће се са улогом цивилног друштва у промовисању дигиталне безбедности са аспекта заштите индивидуалних корисника ИКТ, посебно деце и омладине. Усвојиће знања о улози приватног сектора у заштити националне информационе инфраструктуре. Разумеће међусобну повезаност различитих нивоа заштите националне информационе инфраструктуре и непоходност мултидисциплинарног приступа у изучавању дигиталне безбедности. Студенти ће стећи основна знања о појму вештачке интелигенције и интелигентној анализи података. Разумеће проблеме везане за класификацију, претрагу, екстракцију и анализу велике количине података (Big data). Упознаће се са феноменом Интернет ствари (Internet of Things) и проблемима заштите „паметних ентитета“, као и основним алатима и средствима заштите ИКТ инфраструктуре. Разумеће повезаност тренда дигитализације података са проблемима заштите приватности корисника, а посебно података о личности. Стећи ће знања из области превенције и циљане едукације у подизању безбедносне културе у предметној области и значају дигиталне форензике у прикупљању и чувању дигиталних доказа.

Исход предмета

На крају учења студенти ће поседовати знања о различитим дисциплинарним приступима у изучавању дигиталне безбедности, моћи ће да разумеју њихову међусобну повезаност, као и да препознају методолошке проблеме повезане са овим приступима. Моћи ће да разумеју комплексан феномен сајбер претњи, да објасне њихове узроке, карактеристике, врсте и начине испољавања. Биће у стању да сагледају однос моћи и власти у сајбер простору, те да анализирају конкретне конфликтне ситуације у сајбер простору, да идентификују елементе њихове структуре и коришћене стратегије, те да критички сагледају аргументе учесника у конфликту – процењују њихове конкретне интересе и вредности. Моћи ће да класификују сајбер нападе на основу коришћених алата и техника извршења, мотивације и циљева нападача. Студенти ће бити оспособљени за критичку анализу односа између савремених технолошких решења за дигиталну безбедност (укључујући и вештачку интелигенцију) и актуелних ризика, изазова и претњи, те процену и предикцију последица испољавања сајбер претњи по безбедност држава, корпорација и индивидуалних корисника ИКТ ресурса.

Садржај предмета

Теоријска настава

1. **Концепт дигиталне безбедности**: појмовно одређење информационе и сајбер безбедности, етимологија сајбер безбедности, појмовно одређење сајбер ризика и претњи, појмовно одређење критичне информационе инфраструктуре, индивидуални, корпоративни, национални, регионални и глобални аспекти сајбер безбедности
2. **Безбедност у дигиталном добу**: студије безбедности, безбедносне парадигме и проблем научне анализе и обухвата нових безбедносних појава узрокованих развојем информационо-комуникационих технологија, глобализација и улога приватног и јавног сектора у сајбер безбедности
3. **Друштвени сукоби у дигиталном добу**: сајбер ратовање, сајбер тероризам, тероризам на интернету, сајбер активизам, сајбер шпијунажа, хактивизам
4. **Високотехнолошки криминал:** феноменологија високотехнолошког криминала, узроци, врсте и начини извршења, домаћа и међународна норматива

5. **Стратешки оквир сајбер безбедности**: сајбер суверенитет**,** националне доктрине и стратегије сајбер безбедности, офанзивне и дефанзивне активности националних армија у сајбер простору, иницијатива за постизање сајбер детанта.
6. **Дигитална безбедност и цивилно друштво**: институционални провајдери дигиталне безбедности, активности и мере за постизање и очување дигиталне безбедности индивидуалних корисника ИКТ
7. **Корпоративна безбедност у дигиталном добу**: управљање ризиком од сајбер претњи, активности, мере и стандарди заштите података у ИКТ системима и очувања репутације
8. **Увод у вештачку интелигенцију:** основе вештачке интелигенције, историја вештачке интелигенције, вештачка интелигенција данас, ризици и предности вешачке интелигенције
9. **Велики подаци – Big Data**: увод, карактеристике, различити типови података
10. **Технике анализе велих података – Data Mining**
11. **Технике анализе великих података**: машинско учење, сематничка анализа, визуална анализа
12. **Пример: студије случаја**
13. **Интернет ствари – IoT**
14. **Превентива у сајбер безбедности – Digital Awareness**

Практична настава

1. Дебате на тему методологије процена безбедносних ризика у рачунарским системима и стандарда заштите ИКТ система
2. Дебате на тему стратешког и правног оквира заштите сајбер простора
3. Дебате на тему нових појавних облика сајбер претњи и последица по индивидуалну, корпоративну, националну, регионалну и глобалну безбедност
4. Практичан рад који подразумева примену софтверских алата за анализу и визуализацију података у циљу бољег разумевања тема обухваћених теоријском наставом.

Литература

Обавезна:

Clarke, R., Knake, R. (2010). Cyber war. New York: HarperCollins

Младеновић, Д. (2012). *Међународни аспект сајбер ратовања*. Београд: Медија центар „Одбрана“.

Metz, S. (2000). Armed Conflict In The 21st. Century: The Information revolution And Post-modern Warfare. Carlisle, PA: Strategic Studies Institute, U.S. Army War College.

Chen, H. (2011). Dark web: Exploring and data mining the dark side of the web, (Vol. 30). Springer Science & Business Media.

Kovacevic, A., & Nikolic, D. (2015). Cyber attacks on critical infrastructure: Review and challenges. In *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (pp. 1-18). Hershey: IGI Global.

Милошевић, М. и Путник, Н. (2017). Сајбер безбедност и заштита од високотехнолошког криминала у Републици Србији – стратешки и правни оквир, *Култура полиса*, *33*, 177-191.

Putnik, N., & Milosevic, M. (2018). Trends in Peace Research – Can Cyber Détente Lead to Lasting Peace? In: Cook, B. (editor), *Handbook of Research on Examining Global Peacemaking in the Digital Age*. (pp. 1-19). Hershey: IGI Global.

Russell, S., & Norvig, P. (2020). *Artificial Intelligence: A Modern Approach*, 4th Edition.

Путник, Н., Милошевић, М. и Бошковић, М. (2017). Стратешко планирање сајбер одбране – ка адекватнијем правном оквиру и новој концепцији процене ризика, изазова и претњи, *Војно дело*, 69(7), 174-185.

Schneier, B. (2018). *Click here to kill everybody: Security and survival in a hyper-connected world*. WW Norton & Company.

Erl, T., Khattak, W., & Buhler, P. (2016). *Big Data Fundamentals: Concepts, Drivers & Techniques*. Prentice Hall Press.

Изборна

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company.

Ранђеловић, Д. (2013). *Високотехнолошки криминал*. Београд: Криминалистичко-полицијска академија.

Ковачевић, А., Николић, Д., Поповић, Б. (2017). Internet of Things и проблем приватности, Зборник сажетака на Првој научној конференцији "Урбана безбедност и урбани развој", Београд, 21. 6. 2017.

Kešetović, Ž. & Putnik, N. (2013), “Cyber security” and "Cyber warfare”. In: Penuel, K.B., Statler, M. and Hagen, R. (Eds.), *Encyclopedia of Crisis Management*, Vol. 1., SAGE Publications, 217-219, 219-221.

Путник, Н. (2009). *Сајбер простор и безбедносни изазови*. Београд: Факултет безбедности.

Kešetović, Ž., Putnik, N. & Rakić, M. (2013). Possibilities of Improving Critical Infrastructure Protection in Countries in Transition. U: Dimitrijević, I. (editor), *National Critical Infrastructure Protection – Regional Perspective*. (pp. 131-142). Beograd: Univerzitet u Beogradu – Fakultet bezbednosti i Institut za korporativnu bezbednost – Ljubljana.

Број часова активне наставе: 20	**Теоријска настава: 5**	**Студијски истраживачки рад: 15**

Методе извођења наставе

Предавања, вежбе, презентације, израда семинарског рада, радионице.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	поена	**Завршни испит**	поена
активност у току предавања	**5**	писмени испит	
практична настава	**5**	усмени испт	**60**
колоквијум-и		.....	
семинар-и	**30**		

Начин провере знања могу бити различити наведено у табели су само неке опције: (писмени испити, усмени испт, презентација пројекта, семинари итд.....

*максимална дужна 2 странице А4 формата