План рада на наставном предмету
Назив предмета : **Сајбер безбедност**

Шифра предмета	Статус предмета	Семестар	Број кредита	Фонд часова
СБ.4.34/1.И.СА	Изборни	VIII	5	45+15

Циљеви предмета	Студенти се упознају са основним концептима, терминологијом, изазовима, технологијом, као и потребним вештинама, при чему се комбинују теоретски модели са практичним актуелним примерима. Представљене су актуелни напади као и могућност заштите од њих у свету где је повезано више милијарди нових уређаја. Поред тога студенти се упознају са актуелним стандардима у систему менаџмента безбедношћу информација и сајбер безбедности.
Исход предмета	Студенти ће моћи да разумеју основне принципе сајбер безбедности, као и да идентификују кључне рањивости, претње и нападе у сајбер простору као и могућност њиховог смањивања. Поред тога студенти ће бити упознати са основним стандардима у систему менаџмента безбедношћу информација и сајбер безбедности.
Садржај и структура предмета	1) Увод 2) Основни принципи безбедности информација 3) Анализа напада у рачунарским системима 4) Хакери, етички хакери, етички кодекс. 5) Интернет преваре, крађа идентитета, сајбер ухођење и заштита 6) Злонамерни програми (разумевање, начина ширења и приказ познатих злоанермих програма) 7) Заштита од злонамерних програма 8) Напад одбијања услуга 9) Хакерске технике 10) Стандарди безбедности информација 11) Дигитална форензика

П Р Е Д А В А Њ А		
недеља	Тематска јединица	број часова
I	Уводно предавање	3
II	Основни принципи безбедности информација.	3
III	Анализа напада у рачунарским системима	3
IV	Ризик у рачунарским системима	3
V	Хакери, етички хакери, етички кодекс.	3
VI	Интернет преваре, крађа идентитета, сајбер ухођење, сајбер злостављање и заштита	3
VII	Злонамерни програми (разумевање, начина ширења и приказ познатих злоанермих програма)	3
VIII	Злонамерни програми (разумевање, начина ширења и приказ познатих злоанермих програма) наставак	3
IX	Заштита од злонамерних програма	3
X	Напад одбијања услуга	3
XI	Дигитална форензика	3
XII	Стандарди SRPS ISO/IEC 27XXX	3
XIII	Стандарди SRPS ISO/IEC 27XXX	3
XIV	Вештачка интелигенција и сајбер безбедност	3
XV	Вештачка интелигенција и сајбер безбедност	3

В Е Ж Б Е		
недеља	Тематска јединица	број часова
I	Провера лозинке и креирање ефикасне лозинке	1
II	Криптографија: коришћење софтвера за криптографију.	1
III	Стеганографија: основни елементи и коришћење софтвера за стеганографију.	1
IV	Анализа социјалних мрежа: основни елементи анализе	1
V	Софтвер за анализу социјалних мрежа	1
VI	Анализа социјалне мрежа - пример	1
VII	Сајбер насиље	1
VIII	Сајбер хигијена	1

IX	Злонамерни програми - примери	1
X	Злонамерни програми - примери	1
XI	Хакерске технике	1
XII	Дигитална форензика	1
XIII	Стандарди SRPS ISO/IEC 27XXX	1
XIV	Вештачка интелигенција и сајбер безбедност	1
XV	Вештачка интелигенција и сајбер безбедност	1

Облици извођења наставе	Предавања, вежбе, колоквијум	
Начин оцењивања на предмету	**предиспитне обавезе** до 30: активност на настави, домаћи. **испит** до 70 поена	
Литература	обавезна	Easttom, C. (2020) Computer Security Fundamentals, 4th, Pearson
	допунска	Раковић, Р. (2017) Безбедност информација: основе и смернице, Академска мисао, Београд SRPS ISO/IEC 27032:2019 Информационе технологије – Технике безбедности – Смернице за сајбер безбедност, Београд : Институт за стандардизацију Србије, 2019. Јевремовић, А., Веиновић, М., Шарац, М., Шимић, Г. (2018) Заштита у рачунарским мрежама, Универзитет Сингидунум, Београд.
Подаци о наставницима и сарадницима на предмету	**доц. др Ана Ковачевић** E-mail: ана.ковачевић@fb.bg.ac.rs	

Оквирна питања:

1. Шта је безбедност рачунарског система?
2. Због чега је важно управљање безбедношћу информација?
3. Који су основни циљеви управљања безбедношћу информација?
4. Расположивост информатичких ресурса
5. Поверљивост информатичких ресурса
6. Интегритет информатичких ресурса
7. Којим претњама могу бити изложени информатички ресурси?
8. Какве претње би требало узети у обзир када је у питању систем комуницирања?
9. Шта се подразумева под управљањем безбедношћу информација?
10. Ризик рачунарског система
11. Принципи безбедности информација.
12. Које су основне категорије напада на рачунарске системе?
13. Шта је контрола приступа у контексту безбедности информација?
14. Подела контроле приступа на основу циљева.
15. Подела контроле приступа на основу мера примене.
16. Шта је административна контрола приступа?
17. Шта је техничка контрола приступа?
18. Шта је физичка контрола приступа?
19. Основни сервиси контроле приступа.
20. Провера идентитета.
21. Лозинка
22. Биометрија
23. Токени
24. Методологија контроле приступа.
25. Методи напада у рачунарски систем.
26. Подела контрола приступа према обавезности.
27. Евалуација и тестирање контроле приступа.
28. Улога државе у функцији заштите информатичких ресурса.
29. Компјутерски криминалитет.
30. Сајбер криминал
31. Компјутерски тероризам
32. Значај међународне сарадње на правној заштити безбедности информација
33. Кривична дела против безбедности рачунарских података (КЗРС)
34. Кривична дела против интелектуалне својине (КЗРС)
35. Софтвер према законском облику заштите
36. Доктрина поштеног коришћења
37. Када можете имати поверење у сопствене информације?
38. Криптографија
39. Дигитални потпис
40. Дигитални сертификат
41. Стеганографија
42. Основни елементи за стварање он-лине поверења
43. Како се етика уклапа у контексту остваривања безбедности информација?
44. Значај културе безбедности информација када је у питању електронско пословање
45. Какве претње безбедности информација долазе од запослених?

46. Шта је то противправно коришћење услуга и неовлашћено прибављање информација? Социјални инжењеринг
47. Због чега је важно гајити културу безбедности информација?
48. Како се могу неутралисати унутрашње претње?
49. Тестирање заштите (Етичко хакерисање)
50. Етички кодекс Института за компјутерску етику
51. Злонамерни програми
52. Антивирусни програми
53. Крађа интегритета
54. Хакери
55. Firewall
56. Провера безбедности рачунара
57. Анонимност на webu
58. Зашто се поред законске регулативе и техничких механизама за управљање сигурношћу информација инсистира и на примену одговарајућих стандарда, као признатих модела за управљање безбедношћу информација?
59. Стандарди за управљање безбедношћу инфромација
60. Сертификација у области безбедности информација
61. ISO/IEC 27000 група, значај и историјат.
62. SRPS ISO/IEC 27001
63. SRPS ISO/IEC 27002
64. Кружни ток сталног побољшања
65. Регистар информатичких регистара
66. АУДИТ система за управљање безбедношћу информација, карактеристике, подела према клијентима и врстама провера.