СИЛАБУС

«Інформаційний тероризм»

(назва навчальної дисципліни)

Викладач
Зіняк Любомир Васильович
Прізвище, ім'я, по-батькові
Кандидат юридичних наук,
Науковий ступінь, вчене звання
е-пошта: Lubomir.zinyak@ukr.net
телефон: _0686645953, 0503028473
часи роботи: 10.10 - 11.30 щочетверга

Академічний період
_3_семестр 2020__/2021__ н.р.
Академічні години
дні тижня
час проведення за розкладом
Місце проведення
ауд. 264, майдан Свободи, 6, м. Харків
Навчальне навантаження
__3_ кредита ЄКТС, 90 годин

Пререквізити: Вивчення дисципліни передбачає попереднє засвоєння кредитів з міжнародних відносин, міжнародної інформації, основ міжнародних інформаційних відносин, з дисципліни «інформаційне суспільство», теорії та практики комунікацій.

Постреквізити: Основні положення навчальної дисципліни мають застосовуватися при вивченні дисциплін «Інформаційно-аналітична діяльність в міжнародних відносинах», «Концепції та стратегії міжнародної інформаційної безпеки» та інших навчальних дисциплін за вибором здобувача вищої освіти.

Призначення навчальної дисципліни: Дисципліна призначена для магістрів спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії», освітньо-професійна програма «Міжнародна інформаційна безпека».

Мета викладання навчальної дисципліни полягає у формуванні у здобувачів базових знань у сфері протидії інформаційному тероризму як загрози міжнародній та національній безпеці, а також практичних умінь та навичок правильного тлумачення та застосування механізмів інформаційної протидії тероризму, необхідних для їх майбутньої професійної діяльності у галузі міжнародних відносин, зовнішньої політики, міжнародних комунікацій та регіональних студій та при проведенні досліджень.

Цілі курсу:

- формування наступних загальних компетентностей:

ЗК 7. Вміння аргументувати вибір шляхів вирішення завдань професійного характеру, критично оцінювати отримані результати та обґрунтовувати прийняті рішення

ЗК 11. Навички міжособистісної взаємодії ,цінування та повага різноманітності та багато культурності, здатність спілкування з представниками різних професійних груп різного рівня (з експертами з інших галузей / знань, видів діяльності.

- формування наступних фахових компетентностей:

ФК 1. Поглиблені знання про природу, динаміку, принципи організації міжнародних відносин, типи та види міжнародних акторів, сучасні тенденції розвитку світової політики.
ФК 7. Вміння аргументувати вибір шляхів вирішення завдань професійного характеру , критично оцінювати результати і обґрунтовувати прийняті рішення.

2. Заплановані результати навчання:

Згідно з вимогами освітньо-професійної програми матриця відповідності освітнього компонента **ВБ 1.5. «Інформаційний тероризм»,** методів навчання та форм оцінювання, які використовуються, програмним результатам навчання, визначеним освітньо-професійною програмою «Міжнародна інформаційна безпека».

ПРН 1. Фундаментальні знання щодо природи, джерел та напрямів еволюції міжнародних відносин, міжнародної політики, зовнішньої політики держав, стану теоретичних досліджень міжнародних відносин та світової політики.
ПРН 4. Поглиблені знання проблем міжнародної та національної безпеки, міжнародних та інтернаціоналізованих конфліктів, підходів, способів та механізмів забезпечення безпеки у міжнародному просторі та у зовнішній політиці держав.
ПРН 6. Демонструвати системне сприйняття та розуміння положень, які відносяться до галузі знань «Міжнародні відносини» та є складовою професійної практики.
ПРН 11. Визначати та прогнозувати політичні, дипломатичні, безпекові й інші ризики у сфері міжнародних відносин.
ПРН 12. Оцінювати та аналізувати міжнародні та зовнішньополітичні проблеми та ситуації, пропонувати підходи до вирішення таких проблем.

Інформаційні ресурси:
Необхідні
1. Банк Р. О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект / Р. О. Банк. // Інформація і право. - 2016. – №1. - С. 110-116.
2. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок. В. Б. Толубко, В. О. Хорошко, В. О. Толюпа., 2015. - 288 с.
3. Валюшко І. О. Інформаційна безпека України в контексті російсько-українського конфлікту : автореф. дис. на здобуття наук. ступеня канд. політ. наук : спец. 23.00.04 "Дипломатична академія України при МЗС України" / Валюшко І. О. - К., 2018. - 210 с.
4. Глазов О. В. Міжнародний інформаційний тероризм в контексті загроз національній безпеці України |Електронний ресурс) / 0. В. Глазов // Наукові праці. Політологія. – 2012. – Режим доступу до ресурсу: http://lib.chdu.edu.ua/pdf/naukpraci/politics/2012/197-185-15.pdf. (Дата звернення: 22.08.2019)
5. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. Гнатюк. // UkrainianScientificJournalofInformationSecurity. — 2013. — № 2.— С. 118-129.
6. Грицун О. О. Питання міжнародно-правового регулювання інформаційного тероризму. / О.О. Грицун // Часопис Київського університету права. 2014. № 4. С. 312 - 317.
7. Гуцалюк М. Кібертероризм та заходи протидії / М. Гуцалюк. // Протидія терористичній діяльності: міжнародний досвід і його актуальність для України: матеріали міжнародної науково-практичної конференції. (30 вересня 2016 року, м. Київ). К.: Національна академія прокуратури України. - 2016. - С. 86-88.
8. Давиденко М. О. Протидія СБ України терористичній пропаганді у інформаційному середовищі України / М. О. Давиденко. // Актуальні проблеми управління інформаційною безпекою держави: збірник тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.). Київ: Нац. Акад. СБУ,. - 2019. - С. 35-36. Режим доступу до ресурсу: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf (Дата звернення: 22.08.2019).
9. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам / У. Ільницька. //LvivPolytechnicNationalUniversityInstitutionalRepository. — 2016. — № l. — С. 27-32. Режим доступу до ресурсу: http://ena.lp.edu.ua/bitstream/ntb/37314/1/7_31-36.pdf (Дата звернення: 20.08.2019).
10. Конвенція про кіберзлочинність: Міжнародний документ Ради Європи від 23 листопада |Електронний ресурс]. - 2001. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/994_575 (Дата звернення: 22.08.2019).
11. Крупнейшие кибератаки против Украины: с 2014 года. Инфографика. [Електронний ресурс] // Новое время. – 2017. – Режим доступу до ресурсу: https://nv.ua/ukraine/events/krupnejshie-kiberataki-protiv-ukrainy-s-2014-godainfografika-1438924. html. (Дата звернення: 24.05.2019).

12. Крупнейшие кибератаки против Украины: с 2014 года. Инфографика. [Електронний ресурс] // Новое время. – 2017. – Режим доступу до ресурсу: https://nv.ua/ukraine/events/krupnejshie-kiberataki-protiv-ukrainy-s-2014-godainfografika-1438924. html. (Дата звернення: 24.05.2019).
13. Малик Я. Інформаційна безпека України: стан та перспективи розвитку. / Я. Малик [Електронний ресурс] // Ефективність державного управління. 2015. Вип. 44. С. 13- 20. Режим доступу до ресурсу: http://www. lvivacademy.com/vidavnitstvo_1/edu_44/fail/ch_1/3.pdf (Дата звернення: 20.08.2019).
14. Мануйлов Є. М. Роль і місце інформаційної безпеки держави у розбудові сучасної української держави / Є. М. Мануйлов, Ю. Ю. Калиновський. // Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». - 2016. - № 2. - С. 144-153.
15. Матула М. Феномен інформаційного тероризму як загрози національній та міжнародній безпеці [Електронний ресурс] / М. Матула // Науковий блог. Національний університет «Острозька з академія». - 2014. – Режим доступу до ресурсу: https://naub.oa.edu.ua/2014/fenomen-informatsijnoho-teroryzmu-yak-zahrozy-natsionalnij-ta-mizhnarodnij-bezpetsi/ (Дата звернення: 22.08.2019).
16. Мітін В. І. Інформаційний тероризм на сучасній міжнародній арені / В.І. Мітін // Международный научньй журнал «Интернаука». 2017. № 2 (24). 1 т. С. 65-68.
17. Про боротьбу з тероризмом: Закон України від 20.03.2003 № 638-VI[Електронний ресурс] // Верховна Рада – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/638-15 (Дата звернення: 22.05.2019).
18. Про інформацію: Закон України від 02 жовтня 1992 № 2657-XII [Електронний ресуре] // Верховна | Рада України - Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12#n18 (Дата звернення: 20.08.2019).
19. Про Концепцію боротьби з тероризмом в Україні: Указ Президента України від 05 березня 2019 року № 53/2019. [Електронний ресуре] // Верховна Рада України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/53/2019?lang=ru (Дата звернення: 20.08.2019).
20. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII [Електронний ресурсі] // Верховна Рада України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2469-19
(Дата звернення: 20.08.2019).
21. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. [Електронний ресурсі] // Верховна Рада України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19 (Дата звернення: 20.08.2019).
22. Про рішення Ради національної безпеки і оборони України від 06 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 року № 287/2015 [Електронний ресурсі] // Верховна Рада України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/287/2015 (Дата звернення:20.08.2019).
23. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України: Указ Президента України від 15 березня 2016 року № 96/2016#n2 [Електронний ресуре] // Верховна Рада України - Режим доступу до ресурсу: :https://zakon.rada.gov.ua/laws/show/96/201 6#n2 (дата звернення: 22.08.2019).
24. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року 247/2017. № 247/2017[Електронний ресурс] // Верховна Рада України – Режим доступу до ресурсу: :https://zakon.rada.gov.ua/laws/show/47/2017 (Дата звернення: 20.08.2019).
25. Руководство по передовой практике защиты важнейших обьектов неядерной энергетической инфраструктуры: от террористических актов в связи є угрозами, исходящими

из киберпространства (Електронний ресурс) // ОБСЕ. – 2013. – Режим доступу до ресурсу: https://www.osce.org/ru/secretariat/ 110472?download=true (Дата звернення: 22.08.2019).
26. Самые громкие кибер-атаки на критические инфраструктуры [Електронний ресурс] // Habr.. - 2016. – Режим доступу до ресурсу: https://habr.com/ru/company/panda/blog/3 16500/ (Дата звернення: 22.08.2019).
27. Семен Н. Ф. Російські Інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «ПравдаРу» та «Российский диалог»): автореф. дис. на здобуття наук. ступеня канд. наук з соц. комун.: спец. 27.00.01 "Міжнародний економіко - гуманітарний університет імені акад. С. Демянчука; Дніпровьский національний університет імені Олеся Гончара" / Семен Н. Ф. - Рівне, 2018. - 250 с.
28. Ткачук Т. Інформаційна безпека держави в національному законодавстві європейських країн / Т. Ткачук [Електронний ресурс] // VisegradJournalonHumanRights. — 2018 - №1. - С 145-150. — Режим доступу до ресурсу: http://vjhr.sk/archive/2018_1/part 2/24.pdf (Дата звернення: 20.08.2019).
29. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико правовий аналіз / Т. Ткачук [Електронний ресурсі] // Підприємництво, господарство і право. - 2017. - №10 - С. 182-186. – Режим доступу до ресурсу: :http://pgp-journal. kiev.ua/archive/2017/10/38.pdf (Дата звернення: 20.08.2019).
30. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах
Євроінтеграції України : дис. докт. юр. наук : 12.00.07 / Ткачук Т. Ю. ДВНЗ
«Ужгородський національний університет. - Ужгород, 2019. - 487 с.
31. Форос А. В. Інформаційний тероризм як загроза національній безпеці України. /АВ. Форос // Правова держава. 2010. № 12. С. 256-261
32. Фролова 0. М. Роль ООН в системі міжнародної інформаційної безпеки.
Міжнародні віносини [Електронний ресурс] / О. М. Фролова // Міжнародні віносини. Серія «Політичні науки». - 2018. - № 18-19. Режим доступу до ресурсу: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3468 (Дата звернення : 22.08.2019).
33. Основні засоби інформаційного протиборства та інформаційної війни як явища сучасного міжнародного політичного процесу / І. М. Харченко, С. О. Сапогов, В. М. Шамраєва, Л. В. Новікова / Вісник Харківського національного університету імені В. Н. Кразіна. Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм. - 2017. - №б. - С. 77-81. Режим доступу ресурсу: http://international-relationstourism.karazin.ua/themes/irtb/resources/2c5d772b29c5a9e2139a9f6aa96834d0.pdt (Дата звернення 20.08.2019).
34. Яцик Т. П. Особливості інформаційного тероризму як Одного із способів інформаційної війни. / Т. П. Яцик // Науковий вісник Національного університету ДПС України (економіка, право). 2014. № 2(65). С. 55-60.
35. Яцик Т. П. Розслідування інформаційного тероризму та кіберзлочинності (міжнародно-правовий аспект) / Т. П. Яцик // Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія і практика). 2017. Вип. 1 (5). С. 111-115.
36. Directive (Eu) 2016/1148 Of The European Parliament and Of The Council concerning measures for a high common level of security of network and information systemsacross the Union. [Електронний ресурс] // Official Journal of the European Union.. — 2016. —Режим доступу до ресурсу: https://eur-lex.europa.eu/eli/dir/2016/1148/oj} (Дата звернення: 22.05.2019).
37. European Commission. «eEurope - An information society for all» [Електронний ресурс] — Режим доступудо ресурсу: http://europa.eu/rapid/press-release_SPEECH-O1-180_en.htm?locale=ru (Дата звернення: 22.05.2019).
38. Global Cybersecurity Index (GCI) 2018 [Електронний ресурс] // Studies & Research.ITUPublications. — 2019. — Режим доступу до ресурсу: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf(Дата звернення: 22.08.2019).
39. Kumar M. European Union Parliament Under Cyber Attack! / M. Kumar // TheHacker News. March 29, 2011. URL: https://thehackernews.com/201 1/03/curopean-union-parliament-under-cyber.html (Дата звернення: 22.08.2019).

40. Lemos R. Cyberterrorism: The Real Risk. / R. Lemos // Computer Crime ResearchCenter (CCRC). URL: http://www.crime%research.org/library/Robert|.htm (Дата звернення: 22.08.2019)

Додаткові

1. Антонюк В. В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня канд. держ. упр. : спец. 25.00.02 "Національна академія державного управління при Президентові України" / Антонюк В. В. - Київ, 2017. -21 с.
2. Возженников А. В. Международньй терроризм: борьба за геополитическое господство. /А.В. Возженников Зксмо. Москва. 2007. 528 с.
3. Градов А. П. Деятельность Североатлантического союза в сфере кибербезопасности / А.П. Градов // Зарубежное военное обозрение. 2014. Вып. 7. С. 13-16.
4. Григорьев Н. Ю. Современный кибернетический терроризм и его социальные последствия / Н.Ю. Григорьев, З.Б. Родюков // Вестник университета. 2016. № 5. С. 227- 234.
5. Довгань О. Д. Кібертероризм як загроза інформаційному суверенітету держави / О.Д. Довгань, В.Г. Хлань // інформаційна безпека людини, суспільства, держави. № 3 (7). 2011. С. 49-53.
6. Журавель В. Противодействие угрозе кибертерроризма / В. Журавель //Зарубежное военное обозрение. 2018. №5. С. 12-15.
7. Корченко О. Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти / О.Г. Корченко, В.Л. Бурячок, С.О. Гнатюк // Безпека інформації. 2013. Т. 19. № 1. С. 40-45.
8. Лазарев Н. Я. Терроризм как социально-политическоє явление: истоки, формы и динамика развития в современных условиях : дис. канд. політ. наук : 23.00.01 / Лазарев Н. Я. - Москва, 2007. - 172 с.
9. Негодченко В. Основні напрями державної інформаційної політики в Україні / В. Негодченко В. [Електронний ресурсі]// Підприємництво, господарство і право. 2016. № 4. С. 77-81. Режим доступа до ресурса: http://pgp-journal.kiev.ua/archive/2016/04/15.pdf (дата звернення: 20.08.2019).
10. Правовое регулирование борьбы с киберпреступностью, кибертерроризмом и трафиком людей: опыт Европейского союза / Отв. ред. В. Г. Киютин. А. І. Новиков. Бишкек-Москва, 2010. 239 с
11. Хмелевський Р. М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності / Р.М. Хмелевський // Сучасний захист інформації. 2016. № 4. С. 65-70.
12. Широкова-Мурараш О. Г. Кіберзлочинність та кібертероризм як загрозаміжнародній інформаційній безпеці: міжнародно-правовий аспект / О. Г. Широкова- Мурараш, Ю. Р. Акчурін // Інформація і право. - 2011. - №1. - С. 76-81.
13. Collins A. Contemporary Security Studies. 3rd ed. / A. Collins. — United Kingdom: Oxford University Press, 2013. — 478 с.
14. ENISA. Cyber Europe 2018: After Action Report. 2018. Режим доступа до ресурса:https://www.enisa.europa.eu/publications/cyber-europe-2018-after-actionreport (Дата звернення:22.08.2019).
15. Petya Ransomware Outbreak: Here's What You Need To Know, Symantec Security Response. [Електронний ресурс] // Symantec. 24 October, 2017. Режим доступа до ресурсу: https://www.symantec,com/blogs/threat-intelligence/petya-ransomware-wiper (Дата звернення:22.08.2019).

Політика курсу

При вивченні дисципліни «Інформаційний тероризм» необхідно спиратися на конспект лекцій та рекомендовану літературу. Водночас вітається використання інших джерел з альтернативними поглядами на ті чи інші питання задля формування продуктивної дискусії та різнобічного вивчення інформаційних воєн.

Високо оцінюється прагнення здобувачів вищої освіти:

– регулярно відвідувати заняття;
– планомірно та систематично засвоювати навчальний матеріал;
– активно працювати на практичних заняттях: брати участь в обговоренні дискусійних питань та кейсів;
– повною мірою долучатися до активних форм навчання;
– відпрацьовувати пропущені практичні заняття.

В умовах дії карантинних обмежень освітній процес в університеті здійснюється за змішаною формою навчання, а саме:

– дистанційно (за затвердженим розкладом занять) на платформі Zoom проводяться всі лекційні заняття;

– дистанційно на платформі Zoom(http://https://zoom.us/) проводяться практичні, індивідуальні заняття та консультації, контроль самостійної роботи;

– аудиторно (за затвердженим розкладом занять) проводяться 10% практичних та семінарських занять у навчальних групах кількістю до 20 осіб з урахуванням відповідних санітарних і протиепідемічних заходів. Обов'язковою вимогою є дотримання норм академічної поведінки та етики.

Протоколи комунікації

Основними каналами комунікації зі здобувачами є сайт факультету та чат університетської платформи Zoom. Для складання пропусків та письмових робіт може бути використана електронна скринька викладача.

Форми контролю та критерії оцінювання

При вивченні дисципліни застосовується поточний та підсумковий семестровий форми контролю. Також, передбачено обов'язковий контроль засвоєння навчального матеріалу дисципліни, віднесеного на самостійну роботу.

Поточний контроль знань здобувачів проводиться на *практичному занятті у формі усного опитування та навчальної дискусії, виконання тестових завдань, презентацій доповідей (в тому числі за результатами групової роботи), обговорення ситуаційних завдань, захисту рефератів* тощо.

Сума нарахування балів за виконання завдань на практичному занятті складає:

Тема 1 – 8 балів: захист презентацій індивідуальних доповідей – 4 бали, захист презентацій доповідей за результатами групової роботи – 4 бали.

Тема 2 – 8 балів: захист презентацій індивідуальних доповідей – 4 бали, захист презентацій доповідей за результатами групової роботи – 4 бали.

Тема 3 – 8 балів: захист презентацій індивідуальних доповідей – 4 бали, захист презентацій доповідей за результатами групової роботи – 4 бали.

Тема 4 – 8 балів: захист презентацій індивідуальних доповідей – 4 бали, захист презентацій доповідей за результатами групової роботи – 4 бали,

Поточний контроль *самостійної роботи здобувачів проводиться у формі підготовки відповідей за навчальними питаннями теми, підготовки доповідей (в тому числі за результатами групової роботи), підготовки рефератів.*

Сума балів за виконання завдань для самостійної роботи здобувачів складає:

Тема 1 – 7 балів: підготовка відповідей за навчальними питаннями – 4 бали; виконання презентацій індивідуальних доповідей – 3 бали.

Тема 2 – 7 балів: підготовка відповідей за навчальними питаннями – 4 бали; виконання індивідуальних презентацій доповідей – 3 бали.

Тема 3 – 7 балів: підготовка відповідей за навчальними питаннями – 4 бали; виконання презентацій індивідуальних доповідей – 3 бали;

Тема 4 – 7 балів: підготовка відповідей за навчальними питаннями – 4 бали; виконання презентацій індивідуальних доповідей – 3 бали;

Схема нарахування балів зазначена в таблиці. Загальна сума балів за виконання завдань для самостійної роботи, роботу на практичних заняттях може сягати 60 балів

У разі використання заборонених джерел на заліку здобувач на вимогу викладача залишає аудиторію та одержує загальну нульову оцінку (0 балів). У разі настання / подовження дії **обставин непоборної сили** (в тому числі запровадження жорстких карантинних обмежень в умовах пандемії з забороною відвідування ЗВО) здобувачам вищої освіти денної та заочної форм навчання надається можливість скласти **залік на дистанційній платформі Zoom** в дистанційному курсі «Інформаційний тероризм». режим доступу:
https://us04web.zoom.us/j/6429687377?pwd=dGJxSXozZXQrUUJSbDViQXJlOGttdz09**8.**

Сумарна кількість рейтингових балів за вивчення дисципліни за семестр розраховується як сума балів, отриманих за результатами поточного контролю, балів, отриманих за виконання контрольної роботи, та балів, отриманих за результатами підсумкового семестрового контролю. Максимальна сума балів за семестр складає 100 балів.

Схема нарахування балів

Поточний контроль (загальний бал за темами), з якого				**РАЗОМ**	**ЗАЛІК**	**СУМА**
Т1	Т2	Т3	Т4			
15	**15**	**15**	**15**	**60**	**40**	**100**
на практичних заняттях (бали)						
8	**8**	**8**	**8**			
самостійна робота (бали)						
7	**7**	**7**	**7**			

Т1-Т4 – теми розділів;

Критеріями оцінювання знань за поточний контроль є успішність освоювання знань та набутих навичок на лекціях та семінарських заняттях, що включає систематичність їх відвідування, здатність здобувача засвоювати категорійний апарат, навички узагальненого мислення, логічність та повноту викладання навчального матеріалу, навички творчо підходити до вирішення поставлених завдань, активність роботи на семінарських заняттях, рівень знань за результатами опитування на семінарських заняттях, самостійне опрацювання тем у цілому чи окремих питань.

Контроль засвоєння навчального матеріалу дисципліни, віднесеного на самостійну роботу у формі виконання контрольної роботи, здійснюється шляхом її приймання.

Схема нарахування балів за одне теоретичне питання залікового білету:

- 9-10 балів - здобувач цілком і всебічно розкрив сутність питання, вільно оперує поняттями і термінологією, демонструє глибокі знання джерел, має власну точку зору стосовно відповідних питань і може аргументовано її доводити;

- 7-8 балів - здобувач розкрив сутність питання, вільно оперує поняттями і термінологією, але спостерігаються деякі упущення при відповідях на питання та неточні обґрунтування;

- 5-6 балів - здобувач розкрив питання у загальних рисах, розуміє їхню сутність, намагається робити висновки, але слабко орієнтується в джерелах, припускається помилок, матеріал викладає нелогічно;

- 0-4 балів - здобувач не розкрив питання навіть у загальних рисах, не розуміє його сутності, не орієнтується в джерелах, припускається грубих помилок, матеріал викладає нелогічно.

Набрана кількість рейтингових балів є основою для оцінки за національною шкалою. Шкала оцінювання наведена нижче.

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка
	для дворівневої шкали оцінювання
90–100	зараховано
70-89	зараховано
50-69	зараховано
1-49	не зараховано

КАЛЕНДАР КУРСУ

«Інформаційний тероризм»

№ тижня (дні тижня)	Тема	Форми організації навчання	Кількість годин	Завдання для самостійної роботи
3_ семестр 2020/2021 навчального року				
1 четвер 10.10	**Тема 1. Феномен інформаційного тероризму як загрози міжнародній та національній безпеці.** Тероризм як явище. Закон України «Про боротьбу з тероризмом» від 20.03.2003 року №638. Поняття міжнародного тероризму. Складові терористичної дії (суб'єкт. об'єкт, причина і мотив, мета здійснення, часові та просторові характеристики. використовувані інструменти (засоби), наслідки). Поняття «інформаційний тероризм» та його характерні риси. Суб'єкти інформаційного тероризму. Характерні риси терористичних актів в інформаційній сфері. Види інформаційного тероризму (інформаційно-психологічний тероризм, інформаційно-технічний тероризм). Медіа-тероризм, його характерні риси та способи здійснення. Кібертероризм, його характерні риси, види та способи здійснення. Види правопорушень в інформаційній сфері (правопорушення проти цілісності та доступності	Лекція	2	Ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою.

	комп'ютерних даних і систем: правопорушення, пов'язані з комп'ютерами; правопорушення, пов'язані зі змістом: правопорушення, пов'язані з порушенням авторських та суміжних прав).			
2 четвер 10.10	**Тема 1. Феномен інформаційного тероризму як загрози міжнародній та національній безпеці.** Тероризм як явище. Закон України «Про боротьбу з тероризмом» від 20.03.2003 року № 638. Поняття міжнародного тероризму. Складові терористичної дії (суб'єкт. об'єкт, причина і мотив, мета здійснення, часові та просторові характеристики. використовувані інструменти (засоби), наслідки). Поняття «інформаційний тероризм» та його характерні риси. Суб'єкти інформаційного тероризму. Характерні риси терористичних актів в інформаційній сфері. Види інформаційного тероризму (інформаційно-психологічний тероризм, інформаційно-технічний тероризм). Медіа-тероризм, його характерні риси та способи здійснення. Кібертероризм, його характерні риси, види та способи здійснення. Види правопорушень в інформаційній сфері (правопорушення проти цілісності та доступності комп'ютерних даних і систем: правопорушення, пов'язані з комп'ютерами; правопорушення, пов'язані	Практичне заняття	2	Ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою. Підготувати інформаційні повідомлення, презентації та доповіді за питаннями теми практичного заняття, відповісти на запитання для контролю знань, підготувати завдання за темою, бути готовими до письмового експрес - опитування

	зі змістом: правопорушення, пов'язані з порушенням авторських та суміжних прав).			
3 четвер 10.10	**Тема 2. Світовий досвід протидії інформаційному тероризму.** Протидія інформаційному тероризму в рамках міжнародних організацій та форумів. Протидія інформаційному тероризму в рамках ООН. Глобальна контртерористична стратегія ООН 2006 року. Протидія інформаційному тероризму в рамках НАТО. Роль Інтерполу у протидії інформаційному тероризму. Угода між урядами держав-членів Шанхайської організації співробітництва про співробітництво у сфері забезпечення міжнародної інформаційної безпеки від 16.06.2009 року. Концептуальні підходи до питання інформаційного тероризму, що закріплені в концепції Конвенції про забезпечення міжнародної інформаційної безпеки, представленої у Лондоні у 2011 р. На Конференції з питань кіберпростору, та у проекті «Загального договору з питань кібербезпеки та кіберзлочинності», так званому Договорі Шольберга. Періодизація превентивних заходів та контрзаходів світової спільноти у сфері протидії інформаційному тероризму. Механізми протидії інформаційному тероризму в США. Механізми протидії інформаційному тероризму в провідних державах Азії.	Лекція	2	Ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою.

	Тема 2. Світовий досвід протидії інформаційному тероризму. Протидія інформаційному тероризму в рамках міжнародних організацій та форумів. Протидія інформаційному тероризму в рамках |ООН. Глобальна контртерористична стратегія ООН 2006 року. Протидія інформаційному тероризму в рамках НАТО. Роль Інтерполу у протидії інформаційному тероризму. Угода між урядами держав-членів Шанхайської організації співробітництва про співробітництво у сфері забезпечення міжнародної інформаційної безпеки від 16.06.2009 року. Концептуальні підходи до питання інформаційного тероризму, що закріплені в концепції Конвенції про забезпечення міжнародної інформаційної безпеки, представленої у Лондоні у 2011 р. На Конференції з питань кіберпростору, та у проекті «Загального договору з питань кібербезпеки та кіберзлочинності», так званому Договорі Шольберга. Періодизація превентивних заходів та контрзаходів світової спільноти у сфері протидії інформаційному тероризму. Механізми протидії інформаційному тероризму в США. Механізми протидії інформаційному тероризму в провідних державах Азії.	Практичне заняття	2	Ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою. Підготувати інформаційні повідомлення, презентації та доповіді за питаннями теми практичного заняття, відповісти на запитання для контролю знань, підготувати завдання за темою, бути готовими до письмового експрес - опитування
4/5 четвер 10.10	**Тема 3. Механізми протидії інформаційному тероризму держав Європи .**	Лекція	4	Ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою.

	Засоби протидії інформаційному тероризму держав Європи на регіональному рівні. Поняття регіональної системи безпеки. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 року. Роль ОБСЄ у протидії інформаційному тероризму держав Європи. Хартія європейської безпеки 1999 року. Рішення Ради Міністрів ОБСЄ № 3/04 «Боротьба з використанням Інтернету в терористичних цілях» 2004 року. Рішення Ради Міністрів ОБСЄ Ме 7/06 «Протидія використанню Інтернету в терористичних цілях» 2006 року. Протидія інформаційному тероризму в рамках ЄС. Ініціатива «Електронна Європа». Роль Агентства з мереж інформаційної безпеки (ЕМІЗА) у боротьбі з інформаційним тероризмом. Команда Реагування на Комп'ютерні надзвичайні події ЄС (СЕКТ ЕП). Європейський центр по боротьбі з кіберзлочинністю (ЕС3). Стратегія кібербезпеки ЄС 2013 року. Директива 2016/1148 про заходи для забезпечення високого рівня безпеки мережевих та інформаційних систем у ЄС від 06.07.2016 року. Роль Євроюсту та Європолу у протидії інформаційному тероризму у державах Європи. Засоби протидії інформаційному тероризму держав Європи на національному рівні. Досвід Естонії та Литви у боротьбі з інформаційним тероризмом. Особливості			

	протидії інформаційному тероризму у Великій Британії, Німеччині, Бельгії, Франції та Іспанії Досвід протидії інформаційному тероризму у Туреччині.			
5/6 четвер 10.10	**Тема 3. Механізми протидії інформаційному тероризму держав Європи .** Засоби протидії інформаційному тероризму держав Європи на регіональному рівні. Поняття регіональної системи безпеки. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 року. Роль ОБСЄ у протидії інформаційному тероризму держав Європи. Хартія європейської безпеки 1999 року. Рішення Ради Міністрів ОБСЄ № 3/04 «Боротьба з використанням Інтернету в терористичних цілях» 2004 року. Рішення Ради Міністрів ОБСЄ Ме 7/06 «Протидія використанню Інтернету в терористичних цілях» 2006 року. Протидія інформаційному тероризму в рамках ЄС. Ініціатива «Електронна Європа». Роль Агентства з мереж інформаційної безпеки (ЕМІЗА) у боротьбі з інформаційним тероризмом. Команда Реагування на Комп'ютерні надзвичайні події ЄС (СЕКТ ЕП). Європейський центр по боротьбі з кіберзлочинністю (ЕС3). Стратегія кібербезпеки ЄС 2013 року. Директива 2016/1148 про заходи для забезпечення високого рівня безпеки мережевих та інформаційних систем у ЄС від	Практичне заняття	4	Ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою. Підготувати інформаційні повідомлення, презентації та доповіді за питаннями теми практичного заняття, відповісти на запитання для контролю знань, підготувати завдання за темою, бути готовими до письмового експрес - опитування

	06.07.2016 року. Роль Євроюсту та Європолу у протидії інформаційному тероризму у державах Європи. Засоби протидії інформаційному тероризму держав Європи на національному рівні. Досвід Естонії та Литви у боротьбі з інформаційним тероризмом. Особливості протидії інформаційному тероризму у Великій Британії, Німеччині, Бельгії, Франції та Іспанії Досвід протидії інформаційному тероризму у Туреччині.			
7 четвер 10.10	**Тема 4. Інформаційний тероризм як загроза національній безпеці.** Періодизація та види терористичних атак на інформаційний простір та кіберпростір України. Основні положення Законів України: «Про інформацію» № 2657-XI від 2 жовтня 1992 року, «Про національну безпеку» № 2469-УПІ від 21 червня 2018 року. «Про основні засади забезпечення кібербезпеки України» № 2163-МІ від 5 жовтня 2017 року. «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 5 липня 1994 року. Основні положення Указу Президента України від 25 лютого 2017 року № 247/2017 «Про рішення Радинаціональної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Основні положення Указу Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України	Лекція	2	Ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою.

	від 27 січня 2016 року «Про Стратегію кібербезпеки України ». Роль Служби безпеки України та Кіберполіції України у боротьбі з інформаційним тероризмом. Діяльність Команди реагування на комп'ютерні надзвичайні події в Україні (СЕВТ-Ї А) у сфері протидії інформаційному тероризму. Діяльність Державного центру кіберзахисту та протидії кіберзагрозам (ДЦКЗ) в Україні у боротьбі з інформаційним тероризмом. Співробітництво України з міжнародними організаціями у сфері протидії інформаційному тероризму.			
8 четвер 10.10	**Тема 4. Інформаційний тероризм як загроза національній безпеці** Періодизація та види терористичних атак на інформаційний простір та кіберпростір України. Основні положення Законів України: «Про інформацію» № 2657-XI від 2 жовтня 1992 року, «Про національну безпеку» № 2469-УПІ від 21 червня 2018 року. «Про основні засади забезпечення кібербезпеки України» № 2163-МІ від 5 жовтня 2017 року. «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 5 липня 1994 року. Основні положення Указу Президента України від 25 лютого 2017 року № 247/2017 «Про рішення Радинаціональної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Основні положення Указу	Практичне заняття	2	Ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми практичного заняття, відповісти на запитання для контролю знань, підготувати завдання за темою.

	Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Роль Служби безпеки України та Кіберполіції України у боротьбі з інформаційним тероризмом. Діяльність Команди реагування на комп'ютерні надзвичайні події в Україні (СЕВТ-Ї А) у сфері протидії інформаційному тероризму. Діяльність Державного центру кіберзахисту та протидії кіберзагрозам (ДЦКЗ) в Україні у боротьбі з інформаційним тероризмом. Співробітництво України з міжнародними організаціями у сфері протидії інформаційному тероризму.			