МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Інформаційна безпека держави

Рівень вищої освіти другий (магістерський)
Галузь знань Інформаційні технології

Розглянуто на засіданні кафедри
Протокол №17 від 29 червня 2022 р.

КРОПИВНИЦЬКИЙ – 2022

1. Загальна інформація

Назва курсу	Інформаційна безпека держави
Викладачі та їх профайли	*лектор* – Доренський Олександр Павлович, канд. техн. наук, доцент кафедри кібербезпеки та програмного забезпечення http://kbpz.kntu.kr.ua/dorensky-oleksandr/ https://scholar.google.com/citations?user=0dSLtRgAAAAJ&hl=uk https://publons.com/researcher/2899776/oleksandr-dorenskyi/ https://orcid.org/0000-0002-7625-9022 *асистент* – Резніченко Віталій Анатолійович, викладач кафедри кібербезпеки та програмного забезпечення http://kbpz.kntu.kr.ua/reznichenko-vitaliy/ https://scholar.google.com/citations?hl=uk&user=QN1me_8AAAAJ
Контактний телефон	служб. (0522) 390-449
Е-пошта	bmkntu@ukr.net
Телеграм	https://t.me/ODorenskyi
Фейсбук	www.fb.com/o.dorensky
Консультації	*очні* – відповідно до затвердженого графіку консультацій; *онлайн* – вебінари на платформах Zoom, Discord, Google Meet, е-листування, у месенджерах Fb і T.me

2. Анотація

Навчальна дисципліна “Інформаційна безпека держави” спрямована на здобуття студентами важливих професійних компетентностей, які дадуть можливість організувати запобігання, своєчасне виявлення, припинення чи нейтралізацію реальних і потенційних загроз інформаційній безпеці країни. Це досягається набуттям усталеного розуміння та ґрунтовних фахових навичок аналізу й оцінювання ефективності чинних нормативно-правових документів, законодавчих актів, наявної практики регулювання суспільних відносин у сфері інформаційної безпеки.

Опанувавши курс, здобувачі вищої освіти будуть ґрунтовно знати й розуміти національні інтереси держави в інформаційній сфері, джерела загроз та нормативно-правові документи у сфері забезпечення інформаційної безпеки України, завдання і систему суб’єктів забезпечення інформаційної безпеки України, а також вмітимуть оцінювати ефективність нормативно-правової бази щодо забезпечення інформаційної безпеки держави, практично реалізовувати методи забезпечення інформаційної безпеки країни, розробляти інформаційне забезпечення зв’язків з громадськістю у секторі безпеки, концепції суспільних зв’язків у секторі безпеки, методи й прийоми “чорного” піару, “чорної” риторики, комунікації у сучасних відношеннях, у політиці та секторі безпеки для забезпечення інформаційної безпеки держави.

3. Мета і завдання дисципліни

Метою викладання навчальної дисципліни "Інформаційна безпека держави" є формування у студентів системи ґрунтовних теоретичних знань щодо загроз національній безпеці України в інформаційній сфері, методів та заходів забезпечення інформаційної безпеки держави, зв'язків з громадськістю в секторі забезпечення інформаційної безпеки, чорних маніпулятивних технологій, піару, комунікацій, а також здатності оцінювати і підвищувати ефективність нормативно-правової бази забезпечення інформаційної безпеки держави.

Завданням навчальної дисципліни "Інформаційна безпека держави" є набуття здобувачами вищої освіти за спеціальністю " Комп'ютерні науки " здатності:

- пошуку, оброблення та аналізу інформації;
- застосовувати законодавчу та нормативно-правову базу, а також державні, міжнародні вимоги, практики, з метою забезпечення інформаційної безпеки держави: захисту інтересів громадянина, суспільства й держави в інформаційній сфері;
- використання ІКТ, сучасних методів і моделей інформаційної безпеки.

4. Формат дисципліни

Для денної форми навчання викладання курсу передбачає для засвоєння дисципліни традиційні лекційні заняття із застосуванням електронних презентацій, поєднуючи із лабораторними роботами; формат очний (offline / Face to face).

Для заочної форми навчання – під час сесії формат очний (offline / Face to face), у міжсесійний період – дистанційний (online).

5. Результати навчання

У результаті вивчення навчальної дисципліни "Інформаційна безпека держави" здобувач вищої освіти буде:

знати

національні інтереси держави в інформаційній сфері; джерела загроз інформаційній безпеці держави; сучасний стан інформаційної безпеки держави; завдання із забезпечення інформаційної безпеки держави; система суб'єктів забезпечення інформаційної безпеки України та шляхи її вдосконалення; загальні методи забезпечення інформаційної безпеки держави; забезпечення інформаційної безпеки держави в різних сферах; інформаційне забезпечення зв'язків з громадськістю у секторі безпеки; концепція суспільних зв'язків як системи впливу на людей у секторі безпеки; комунікація й вплив на громадськість у сфері військово-цивільних відносин; майстерність комунікації; чорний ПР та чорна риторика у сучасних відношеннях, у політиці та секторі безпеки; правове регулювання ПР-діяльності;

вміти

готувати пропозиції до нормативних актів і документів з метою забезпечення інформаційної безпеки держави;

аналізувати реалізації прийнятої політики інформаційної безпеки;

професійно виконувати роботу на основі знань сучасних інформаційно-комунікаційних технологій;

володіти соціальними навичками (Soft Skills):

здатність до пошуку, оброблення й аналізу законодавчої та нормативно-правової інформації, яка міститься у базах даних центральних органів виконавчої влади України.

6. Обсяг дисципліни

Вид роботи	Кількість годин, очна / заочна ф. н.
Лекції	56 / 8
Лабораторні заняття	28 / 4
Самостійна робота	96 / 168 та 60 год. підготовки до екзаменів
Разом	*270*

7. Ознаки дисципліни

Рік викладання	Курс (рік навчання)	Семестр	Спеціальність	Кількість кредитів / годин	Кількість змістовних модулів	Вид підсумкового контролю	Нормативна / вибіркова
2022	III	5	122 Комп'ютерні науки	5 / 150	2	екзамен	вибіркова
2023		6		4 / 120	2	екзамен	

8. Пререквізити

Дисципліна "Інформаційна безпека держави" краще опановується після вивчення студентом навчальних дисциплін "Основи комп'ютерних технологій", "Вступ до кібербезпеки", "Бази даних".

9. Технічне й програмне забезпечення / обладнання

Для викладання навчальної дисципліни застосовується матеріально-технічна база кафедри кібербезпеки та програмного забезпечення: мультимедійний проектор Epson EB-X41, спеціалізовані комп'ютерні лабораторії з персональними комп'ютерами Athlon 2.4, (15 шт.), AMD Semprom LE-1150 (18 шт.), Athlon II 215x2 (10 шт.), AMD Duron 1,2 GHz (15 шт.), програмне забезпечення OpenOffice версії 4.1.7 (ліцензія LGPL), Google Chrome версії 80.0.3987.162 (ліцензія EULA), відкрита бездротова мережа Wi-Fi, вільний доступ до Інтернету.

10. Політика курсу

Організація освітнього процесу. Учасники освітнього процесу повинні дотримуватися вимог Положення про організацію освітнього процесу ЦНТУ, Кодексу академічної доброчесності ЦНТУ, Положення про дотримання академічної доброчесності НПП та здобувачами вищої освіти, інших нормативних актів університету http://www.kntu.kr.ua/?view=univer&id=4.

Академічна доброчесність. Очікується, що здобувачі дотримуватимуться Кодексу академічної доброчесності ЦНТУ, усвідомлюючи наслідки її порушення.

Відвідування занять. Очікується, що здобувачі братимуть активну участь у лекційних і лабораторних заняттях курсу, консультаціях. Пропущені заняття повинні бути відпрацьовані не пізніше, ніж за тиждень до екзаменаційно-залікової сесії.

Поведінка на заняттях. Недопустимими є списування, плагіат, несвоєчасне виконання завдань та самостійної роботи, пасивність під час лекційних, лабораторних, консультаційних заняттях. Завдання лабораторних робіт виконуються студентом аудиторно (в комп'ютерній лабораторії згідно з розкладом занять) під керівництвом викладача, при цьому виконуючи порядок виконання завдань лабораторних робіт, який міститься у методичних рекомендаціях до виконання лабораторних робіт з навчальної дисципліни.

Виконання самостійної роботи. Студенти повинні виконувати завдання СРС у визначений термін із обов'язковим обговоренням і представленням результатів на консультаціях. Є недопустимим прострочення реченця (дедлайна) виконання СРС або неявка на консультації без поважних причин. В межах СРС студент зобов'язаний готуватися до лабораторних занять.

11. Навчально-методична карта дисципліни

Тиждень, дата, обсяг годин	Тема, основні питання *(розкривають зміст і є орієнтирами для підготовки до модульного і підсумкового контролю)*	Форма діяльності (заняття) /формат	Матеріали	Література, інформаційні ресурси	Завдання, обсяг годин	Вага оцінки	Термін виконання
Змістовний модуль І. ОБ'ЄКТИ І СУБ'ЄКТИ БЕЗПЕКИ ДЕРЖАВИ В ІНФОРМАЦІЙНІЙ СФЕРІ							
Тиждень 1-2 осіннього семестру, за розкладом занять, 4 год.	**Тема 1** *Національні інтереси держави в інформаційній сфері.* Дефініція держави, безпеки, інформації та поняття забезпечення інформаційної безпеки держави. Концептуальні поняття інформаційної безпеки держави. Правова основа національних інтересів України в інформаційній сфері: Конституція України, Закони України, Доктрина інформаційної безпеки України.	Лекція / Face to face	Презентація	1–5, 10, 12, 19	Самостійно опрацювати теоретичний матеріал теми 1. 6 год.	9	Навчальний тиждень 2 осіннього семестру
Тиждень 3-4 осіннього семестру, за розкладом занять, 4 год.	**Тема 2** *Джерела загроз інформаційній безпеці держави.* Поняття загрози інформаційній безпеці держави та її джерел. Дестабілізуючі фактори інформаційної безпеки держави. Загрози національним інтересам і національній безпеці України. Правове підґрунтя актуальних загроз інформаційній безпеці України та їх джерел. Класифікація загроз ІБД. Загрози інтересам особистості, суспільства і держави. Внутрішні і зовнішні джерела загроз ІБД.	Лекція / Face to face	Презентація	2, 3, 5, 11	Самостійно опрацювати теоретичний матеріал теми 2. 6 год.	9	Навчальний тиждень 4 осіннього семестру
Тиждень 1-4 осіннього семестру, за розкладом занять, 4 год.	**Лабораторна робота 1** *Аналіз нормативно-правових документів у сфері забезпечення інформаційної безпеки України.* Використання бази даних "Законодавство України" для отримання й аналізу чинних нормативно-правових документів у сфері забезпечення інформаційної безпеки держави.	Лабораторне заняття / Face to face	Методичні рекомендації	22	Самостійно опрацювати теоретико практичні питання СРЗВО № 1 – самопідготовка до виконання лабораторної роботи № 1. 2 год.	10	За розкладом лабора-торних занять
Тиждень 5-6 осіннього семестру, за розкладом занять, 4 год.	**Тема 3** *Стан інформаційної безпеки держави. Інциденти в сфері інформаційної безпеки України.* Сучасний стан нормативно-правового забезпечення сфери ЗІБ України. Законодавче й нормативно-правове ЗІБ України. Загальне становище інформаційної безпеки України в сучасних умовах.	Лекція / Face to face	Презентація	3–5, 14, 20, 23, 25, 27	Самостійно опрацювати теоретичний матеріал теми 3. 6 год.	9	Навчальний тиждень 6 осіннього семестру
Змістовний модуль ІІ. СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ							
Тиждень 7-8 осіннього семестру, за розкладом занять, 4 год.	**Тема 4** *Завдання із забезпечення інформаційної безпеки держави*. Основні завдання системи ЗІБД та її суб'єктів. Функції та основні елементи організаційної основи системи ЗІБД. Пріоритети державної політики України в інформаційній сфері. Механізм реалізації завдань із ЗІБД. Актуальні завдання щодо забезпечення інформаційної безпеки України.	Лекція / Face to face	Презентація	5	Самостійно опрацювати теоретичний матеріал теми 4. 6 год.	9	Навчальний тиждень 8 осіннього семестру

Тиждень 5-8 осіннього семестру, за розкладом занять, 4 год.	**Лабораторна робота 2** *Оцінювання ефективності нормативно-правових актів щодо забезпечення інформаційної безпеки держави.* Реалізація підходів і методів оцінювання ефективності чинних нормативно-правових документів у сфері забезпечення інформаційної безпеки держави.	Лабораторне заняття / Face to face	Методичні рекомендації	22	Самостійно опрацювати теоретико-практичні питання СРЗВО № 2 – самопідготовка до виконання лабораторної роботи № 2. 2 год.	9	За розкладом лабораторних занять
Тиждень 9-10 осіннього семестру, за розкладом занять, 4 год.	**Тема 5** *Система суб'єктів забезпечення інформаційної безпеки України та шляхи її вдосконалення.* Поняття системи ЗІБД. Основні суб'єкти та інститути ІБД. Суб'єкти ЗІБ України. Структура системи забезпечення інформаційної безпеки України та компетенція її суб'єктів. Нормативно-правове підґрунтя діяльності суб'єктів ЗІБД. Шляхи вдосконалення системи суб'єктів забезпечення інформаційної безпеки України.	Лекція / Face to face	Презентація	2–5, 7, 11, 13, 18	Самостійно опрацювати теоретичний матеріал теми 5. 6 год.	9	Навчальний тиждень 10 осіннього семестру
Тиждень 11-12 осіннього семестру, за розкладом занять, 4 год.	**Тема 6** *Методики забезпечення інформаційної безпеки.* Основні способи, засоби й прийоми забезпечення інформаційної безпеки. Форми забезпечення безпеки суб'єктів інформаційного процесу. Методи забезпечення інформаційної безпеки держави.	Лекція / Face to face	Презентація	11	Самостійно опрацювати теоретичний матеріал теми 6. 6 год.	9	Навчальний тиждень 12 осіннього семестру
Тиждень 9-12 осіннього семестру, за розкладом занять, 4 год.	**Лабораторна робота 3** *Практична реалізація методів забезпечення інформаційної безпеки.* Реалізація методів забезпечення інформаційної безпеки на різних рівнях захисту.	Лабораторне заняття / Face to face	Методичні рекомендації	22	Самостійно опрацювати теоретико-практичні питання СРЗВО № 3 – самопідготовка до виконання лабораторної роботи № 3. 2 год.	9	За розкладом лабораторних занять
Тиждень 13-14 осіннього семестру, за розкладом занять, 4 год.	**Тема 7** *Загальні методи забезпечення інформаційної безпеки України.* Загальні методи ЗІБД. Особливості забезпечення інформаційної безпеки України в різних сферах.	Лекція / Face to face	Презентація	11	Самостійно опрацювати теоретичний матеріал теми 7. 6 год.	6	Навчальний тиждень 13 осіннього семестру
Змістовний модуль ІІІ. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ У РІЗНИХ СФЕРАХ							
Тиждень 1-2 весняного семестру, за розкладом занять, 4 год.	**Тема 8** *Забезпечення інформаційної безпеки держави в різних сферах.* ЗІБ України у сфері економіки, внутрішньої політики України, в загальнодержавних ІС та ТКС, сфері зовнішньої політики, оборони, у галузі науки й техніки, у сфері культури й духовного життя держави, у правоохоронній і судовій сферах, в умовах надзвичайних ситуацій, міжнародне співробітництво України в галузі ЗІБД.	Лекція / Face to face	Презентація	11	Самостійно опрацювати теоретичний матеріал теми 8. 6 год.	4	Навчальний тиждень _ весняного семестру
Тиждень 3-4 весняного семестру,	**Тема 9** *Інформаційне забезпечення зв'язків з громадськістю у секторі безпеки.* Зв'язки з громадськістю в контексті реалізації державної	Лекція / Face to face	Презентація	8, 21, 27	Самостійно опрацювати теоретичний матеріал теми 9. 6 год.	4	Навчальний тиждень _ весняного

за розкладом занять, 4 год.	політики у сфері інформаційної безпеки. Засоби інформаційно-аналітичного забезпечення служб із зв'язків з громадськістю. Стратегічні комунікації сектору безпеки і оборони. Інформаційне забезпечення зв'язків з громадськістю в секторі безпеки.						семестру
Тиждень 1-4 весняного семестру, за розкладом занять, 4 год.	**Лабораторна робота 4** *Практична реалізація концепції суспільних зв'язків у секторі безпеки.* Організація зв'язків з громадськістю як системи впливу на людей задля досягнення високої суспільної репутації.	Лабораторне заняття / Face to face	Методичні рекомендації	8, 21, 27	Самостійно опрацювати теоретико практичні питання СРЗВО № 4 – самопідготовка до виконання лабораторної роботи № 4. 2 год.	10	За розкладом лабора-торних занять
Тиждень 5-6 весняного семестру, за розкладом занять, 4 год.	**Тема 10** *Концепція суспільних зв'язків як системи впливу на людей у секторі безпеки.* Дефініція суспільства. Основні підходи до розуміння суспільства та соціальна структура суспільства. Сутність і структура суспільних відносин. Суспільні зв'язки та соціальні відносини. Паблік рілейшнз як система впливу на людей у секторі безпеки.	Лекція / Face to face	Презентація	6, 10, 21	Самостійно опрацювати теоретичний матеріал теми 10. 6 год.	4	Навчальний тиждень _ весняного семестру
Змістовний модуль IV. МЕТОДИ Й ЗАСОБИ КОМУНІКАЦІЇ ТА ЗВ'ЯЗКІВ З ГРОМАДСЬКІСТЮ							
Тиждень 7-8 весняного семестру, за розкладом занять, 4 год.	**Тема 11** *Комунікація й вплив на громадськість у сфері військово-цивільних відносин.* Сутність цивільно-військових відносин та особливості їх становлення в Україні. Нормативно-правова база цивільно-військових відносин. Процес комунікації та його елементи. Мета й методи впливу на громадськість.	Лекція / Face to face	Презентація	15, 16, 21	Самостійно опрацювати теоретичний матеріал теми 11. 6 год.	4	Навчальний тиждень _ весняного семестру
Тиждень 5-8 весняного семестру, за розкладом занять, 4 год.	**Лабораторна робота 5** *Практична реалізація метода "чорного" PR.* Реалізація метода "чорного" ПР на структурно-організаційному, змістовому або емоційно-психічному рівні.	Лабораторне заняття / Face to face	Методичні рекомендації	22, 27	Самостійно опрацювати теоретико практичні питання СРЗВО № 5 – самопідготовка до виконання лабораторної роботи № 5. 2 год.	10	За розкладом лабора-торних занять
Тиждень 9-10 весняного семестру, за розкладом занять, 4 год.	**Тема 12** *Майстерність комунікації.* Цілі, функції, етапи комунікації. Моделі комунікації. Види і форми комунікації. Міжособистісті, групові та масові комунікації. Комунікатор як професія.	Лекція / Face to face	Презентація	15–16, 21, 27	Самостійно опрацювати теоретичний матеріал теми 12. 6 год.	4	Навчальний тиждень _ весняного семестру
Тиждень 11-12 весняного семестру, за розкладом занять, 4 год.	**Тема 13** *Чорний ПР та чорна риторика у сучасних відношеннях, у політиці та секторі безпеки.* Поняття й функція чорного PR. Структурно-організаційний, змістовий, емоційно-психічний рівні чорного піару. Чорний PR як сугестивна технологія. Поняття, принципи організації і правила чорної риторики. Чорний ПР і чорна риторика в сучасних відношеннях у політиці та секторі безпеки.	Лекція / Face to face	Презентація	9, 17, 27	Самостійно опрацювати теоретичний матеріал теми 13. 6 год.	4	Навчальний тиждень _ весняного семестру

Тиждень 9-12 весняного семестру, за розкладом занять, 6 год.	**Лабораторна робота 6** *Практична реалізація прийомів "чорної" риторики.* Реалізація прийомів "чорної" риторики як маніпулятивної технології "чорного" ПР на структурно-організаційному, змістовому або емоційно-психічному рівні.	Лабораторне заняття / Face to face	Методичні рекомендації	22	Самостійно опрацювати теоретико практичні питання СРЗВО № 6 – самопідготовка до виконання лабораторної роботи № 6. 2 год.	10	За розкладом лабора-торних занять
Тиждень 13-14 весняного семестру, за розкладом занять, 4 год.	**Тема 14** *Правове регулювання ПР-діяльності.* Правове забезпечення зв'язків з громадськістю, закони та нормативні акти. Нормативно-правова база функціонування PR-служб в Україні.	Лекція / Face to face	Презентація	8, 24, 27	Самостійно опрацювати теоретичний матеріал теми 14. 6 год.	6	Навчальний тиждень _ весняного семестру

12. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю студентів, усне опитування, письмовий контроль, тестовий контроль, захист результатів виконання лабораторних робіт.

Форма підсумкового контролю: екзамен (у осінньому та у весняному семестрах).

Контроль знань і умінь здобувачів (поточний і підсумковий) здійснюється згідно з кредитною трансферно-накопичувальною системою організації освітнього процесу в ЦНТУ. Рейтинг студента із засвоєння дисципліни визначається за 100-бальною шкалою у кожному семестрі: складається із рейтингу з поточної навчальної роботи впродовж весняного семестру для оцінювання якої призначається 60 балів (по 30 балів за кожен змістовний модуль) та семестрового екзамену, на який відведено 40 балів.

Розподіл балів, які здобувають студенти під час вивчення дисципліни

Поточний контроль та самостійна робота у осінньому семестрі							Екзамен	РАЗОМ	Поточний контроль та самостійна робота у весняному семестрі							Екзамен	РАЗОМ
Змістовний модуль I			Змістовний модуль II						Змістовний модуль III			Змістовний модуль IV					
Тема 1	Тема 2	Тема 3	Тема 4	Тема 5	Тема 6	Тема 7			Тема 8	Тема 9	Тема 10	Тема 11	Тема 12	Тема 13	Тема 14		
9	9	9	9	9	9	6	*40*	100	9	9	9	9	9	9	6	*40*	100

Відповідність шкали оцінювання ЄКТС національній системі оцінювання

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою
90-100	A	відмінно
82-89	B	добре
74-81	C	
64-73	D	задовільно
60-63	E	
35-59	FX	незадовільно з можливістю повторного складання
1-34	F	незадовільно з обов'язковим повторним вивченням дисципліни

Критерії оцінювання знань і вмінь здобувачів визначені Положенням про організацію освітнього процесу в ЦНТУ (*стор. 32-33*).

13. Рекомендовані література й джерела

Базова

1. Доренський О. П. Модель поведінки держави в умовах проявів ознак інформаційної експансії, агресії, війни / О. П. Доренський // Інформаційна безпека держави, суспільства та особистості: Всеукр. наук.-практ. конф., 16 кві. 2015 р. : тези доп. – Кіровоград: КНТУ, 2015. – С. 131-133.
2. Інформаційна безпека держави : підруч. для студ. вищ. навч. закл. / Ю.В. Стасєв, О.А. Смірнов, В.В. Бараннік, О.В. Коваленко, О.П. Доренський, О.М. Дрєєв, В.І. Вялкова; за ред. Ю.В. Стасєва; — Кіровоград: РВЛ КНТУ, 2016. — 264 с.
3. Про національну безпеку України : Закон України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19.
4. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України" : Указ Президента України від 26 травня 2015 року № 287/2015. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/287/2015.
5. 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 № 47/2017 . – Режим доступу: http://zakon5.rada.gov.ua/laws/show/47/2017.
6. Пасічник, В. М. Філософська категорія безпеки як основа нової парадигми державного управління національною безпекою [Електронний ресурс] – Демократичне врядування : наук. вісник. – 2011. – Вип. 7. – Режим доступу: http://www.lvivacademy.com/vidavnitstvo_1/visnik7/fail/pasichnyk.pdf.
7. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки / К. Захаренко // Науковий вісник Харківського національного педагогічного університету імені Г. С. Сковороди. – 2017. – Вип. 48(1). – С. 212-219.
8. Тихомирова Є. Б. Зв'язки з громадськістю : навчальний посібник / Є. Б. Тихомирова. – К.: НМЦВО, 2011. – 560 с. (Режим доступу: http://esnuir.eenu.edu.ua/bitstream/123456789/419/1/PR_Tikhomirova.pdf)
9. Копилов В. О. Політичний PR як інструмент позитивного та негативного впливу на політичну активність і електоральний вибір студентів / В. О. Копилов, Л. А. Лобанова // Гуманітарний часопис. – 2017. – № 1. – С. 94-103.
10. Кириченко В.М. Теорія держави і права : Навч. посібник / Кириченко В. М., Куракін О. М. – К.: Центр навчальної літератури, 2010. – 264 с.
11. Богуш В. М. Інформаційна безпека держави : навч. посібник / В. М. Богуш, О. К. Юдін. – К.: МК-Прес, 2005. – 432 с.
12. Корольов М.В. Проблематика дослідження питань інформаційної безпеки у державному управлінні / М.В. Корольов, О.О. Скопа // Вісн. Східноукраїнського нац. ун- ту ім. В. Даля. – 2013. – № 15(1). – С.88-93.
13. Зайцев М.М. Суб'єкти забезпечення інформаційної безпеки України [Електронний ресурс] / М.М. Зайцев // Форум права. – 2013. – № 3. – С. 231 – 238. – Режим доступу:http://nbuv.gov.ua/j-pdf/FP_index.htm_2013_3_40.pdf.
14. Хімей В. Основні сучасні проблеми інформаційної безпеки України / В. Хімей // Теле- та радіожурналістика. – 2014. – Вип. 13. – С.127-132.
15. Партико З. В. Теорія масової інформації та комунікації : Навч. посібник / З. В. Партико. – Львів: Афіша, 2008. - 309 с.
16. Косюк О. М. Теорія масової комунікації : навч. посіб. / О. М. Косюк. – Луцьк: ВНУ ім. Лесі Українки, 2012. – 384 с.
17. Сугестивні технології маніпулятивного впливу : навч. посіб. / [В. М. Петрик, М. М. Присяжнюк, Л. Ф. Компанцева, Є. Д. Скулиш, О. Д. Бойко, В. В. Остроухов]; за заг. ред. Є.Д.Скулиша. – 2-ге вид. / Національна академія Служби Безпеки України. – К.: ВІПОЛ, 2011. – 248 с.

Допоміжна

18. Про Раду національної безпеки і оборони України : Закон України. – Режим доступу: zakon.rada.gov.ua/laws/show/183/98-вр.

19. Олійник О. В. Адміністративно-правові засади інформаційної безпеки / О. В. Олійник // Європейські перспективи. – 2012. – № 4(1). – С. 65-68.

20. Малик Я.Й. Забезпечення інформаційної безпеки України у контексті світового досвіду / Я.Й. Малик, О. І. Береза // Ефективність державного управління. – 2012. – Вип. 32. – С.20-27.

21. Теорія масової комунікації : навч. посіб. / О. М. Косюк. – Луцьк : ВНУ ім. Лесі Українки, 2012. – 384 с.

Інформаційні ресурси

22. Інформаційна безпека держави : система дистанційної освіти ЦНТУ : веб-сайт. – Режим доступу: http://moodle.kntu.kr.ua/course/view.php?id=1540. – Назва з екрана.

23. CERT-UA [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – CERT-UA функціонує в рамках Держспецзв'язку, 2019. – Режим доступу: https://cert.gov.ua/. – Назва з екрану.

24. Законодавство України : Інформаційно-пошукова система [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Верховна Рада України, 1994-2019. – Режим доступу: http://zakon3.rada.gov.ua/laws. – Назва з екрану.

25. Документи : Президент України : Офіційне інтернет-представництво [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Адміністрація Президента України, 2019. – Режим доступу: http://www.president.gov.ua/documents/all. – Назва з екрану.

26. Наукова періодика України [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Національна бібліотека України імені В. І. Вернадського, 2013-2019. – Режим доступу: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv. – Назва з екрану.

27. Навчальні матеріали онлайн [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Навчальні матеріали онлайн (pidruchniki.website), 2010-2019. – Режим доступу: http://pidruchniki.com/. – Назва з екрану.