Силабус курсу:

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВОЛОДИМИРА ДАЛЯ

ІНФОРМАЦІЙНА БЕЗПЕКА

Ступінь вищої освіти:	магістр
Спеціальність:	061 «Журналістика»
Рік підготовки:	1
Семестр викладання:	весняний
Кількість кредитів ЄКТС:	5,5
Мова(-и) викладання:	українська
Вид семестрового контролю	залік

Автор курсу та лектор:

д. філол. н., проф. Глотов Олександр Леонідович

професор кафедри журналістики і українознавчих студій

algall@ukr.net	+38-098-206-89-27	Viber, Telegram	за розкладом
електронна адреса	телефон	месенджер	консультації

Анотація навчального курсу

Мета програми:
засвоєння знань про формування інформаційної безпеки від національного до особистісного рівня та визначення підходів до захисту та розвитку інформаційного простору для всебічного інформаційного розвитку українського суспільства
Завданнями навчальної дисципліни є:
- формування знань щодо концептуальних засад, принципів, форм та методів забезпечення інформаційної безпеки;
- ознайомлення з ключовими загрозами інформаційної безпеки, основами управління інформаційною безпекою;
- вироблення навичок використання знань теорії і практики інформаційної безпеки у практиці публічного управління.

За результатами навчання слухачі повинні демонструвати:
знання:
– концепції електронного урядування та принципів формування електронної держави;
– сутності державної політики України у сфері інформаційної безпеки;
– основних положень законодавства України щодо інформаційної безпеки;
– досвіду зарубіжних країн у здійсненні заходів щодо інформаційної безпеки;
– механізмів та інструментів запобігання загроз в інформаційному просторі для суспільства та особистості;

– принципів формування медіа-імунітету.

уміння:

– аналізувати, узагальнювати й розкривати зміст основних законодавчих та інших нормативно-правових актів щодо електронного урядування та інформаційної безпеки;

– застосовувати норми чинного законодавства, що регулюють інформаційну сферу та інформаційну безпеку в практичній діяльності;

– використовувати механізми та інструменти забезпечення інформаційної безпеки на своєму робочому місці (у ході професійної управлінської діяльності) та в побуті;

навички:

– вивчення кращих практик формування інформаційної безпеки інших країн та вибору їх для реалізації в Україні;

– аналізу та узагальнення інформації щодо різноманітних аспектів (соціальних, економічних, кримінальних, управлінських тощо) формування інформаційної безпеки як управлінської проблеми в органах публічної влади;

– дотримання правил безпечної роботи в Інтернеті з урахуванням принципів інформаційної безпеки;

– аналізу рівня захищеності інформаційних систем органів влади;

– практичного застосування відомих програмних засобів захисту інформації та кібербезпеки.

Компетентності, які дає можливість здобути навчальна дисципліна.

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК03. Здатність генерувати нові ідеї (креативність).

ЗК04. Здатність спілкуватися іноземною мовою як усно, так і письмово.

ЗК05. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК06. Здатність приймати обґрунтовані рішення.

ЗК08. Здатність спілкуватися з представниками інших професійних груп різного рівня.

СК01. Здатність використовувати спеціалізовані концептуальні знання з теорії та історії журналістики, новітні технологічні досягнення для розв’язання задач дослідницького та / або інноваційного характеру у сфері журналістики.

СК02. Здатність критично осмислювати проблеми у сфері журналістики та дотичні до них міждисциплінарні проблеми.

СК03. Здатність приймати ефективні рішення у сфері журналістики.

СК05. Здатність зрозуміло і недвозначно доносити власні висновки з питань журналістики, а також знання та пояснення, що їх обґрунтовують, до фахівців і нефахівців, зокрема до осіб, які навчаються.

Що забезпечується досягненням наступних програмних результатів навчання:

РН01. Приймати ефективні рішення з проблем журналістики, у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог.

РН02. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан та розвиток журналістики.

РН03. Проводити збір, інтегрований аналіз та узагальнення матеріалів з різних джерел, включаючи наукову та професійну літературу, бази даних, та перевіряти їх на достовірність, використовуючи сучасні методи дослідження.

РН04. Вільно спілкуватися державною та іноземною мовами усно і письмово для обговорення професійної діяльності, результатів досліджень та інновацій, пошуку та аналізу відповідної інформації.

РН05. Генерувати нові ідеї та використовувати сучасні технології під час створення медіапродуктів.

РН06. Оцінювати достовірність інформації та надійність джерел, ефективно опрацьовувати та використовувати інформацію для проведення наукових досліджень та практичної діяльності.
РН07. Дискутувати зі складних комунікаційних проблем, пропонувати і обґрунтовувати варіанти їх розв'язання.

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Поняття інформаційної безпеки держави, суспільства та особи
Інформаційна безпека (поняття і визначення). Підходи до визначення поняття «інформаційна безпека». Інтереси особи, суспільства та держави в інформаційній сфері. Об'єкти, суб'єкти та види інформаційної безпеки. Співвідношення понять інформаційної та кібербезпеки.
Тема 2. Загрози інформаційної безпеки.
Характеристика інформаційної безпеки. Класифікація загроз. Сучасні загрози. Інформаційні ризики. Витік інформації.
Тема 3. Принципи, форми та методи забезпечення інформаційної безпеки держави.
Основні принципи забезпечення інформаційної безпеки держави. Основні форми забезпечення інформаційної безпеки держави. Методи забезпечення інформаційної безпеки.
Тема 4. Інформаційна система персональних даних.
Нормативні документи захисту даних. Конфіденційність персональних даних. Захист персональної інформації. Європейська система захисту персональних даних.
Тема 5. Забезпечення безпеки інформації та інформаційних ресурсів.
Основні напрями забезпечення безпеки інформації. Правовий захист. Організаційний захист. Інженерно-технічний захист.
Тема 6. Захист інформаційних систем.
Джерела конфіденційної інформації. Інформаційна система як об'єкт захисту інформації. Рівні захисту інформаційних систем. Аналіз вразливостей корпоративних інформаційних систем. Основні принципи захисту інформації.
Тема 7. Поняття та зміст інформаційного протиборства.
Основні форми інформаційного протиборства. Основні форми інформаційної війни. Інформаційна зброя в інформаційній війні.
Тема 8. Основи управління інформаційною безпекою.
Політика інформаційної безпеки організації. Основні правила інформаційної безпеки організації. Заходи управління інформаційною безпекою.
Тема 9. Інформаційна безпека України
Забезпечення інформаційної безпеки України. Система та політика забезпечення інформаційної безпеки України. Інформаційна безпека України у сфері прав і свобод людини.

БАЗОВА ЛІТЕРАТУРА

1. Інформаційна безпека держави : навч. посіб. / В. М. Рудницький [та ін.] ; Черкас. держ. технол. ун-т. Харків : ДІСА ПЛЮС, 2018. 358 с.
2. Інформаційна безпека держави: навч. посіб. / В. І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с.
3. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.
4. Лизанчук В. В. Інформаційна безпека України: теорія і практика : підручник / Львів. нац. ун-т ім. Івана Франка, Львів. шк. журналістики. Львів : ЛНУ ім. Івана Франка, 2017. 725 с.

5. Панченко О. А. Інформаційна безпека в епоху турбулентності: державно-управлінський аспект : монографія. Київ : КВІЦ, 2020. 331 с.
6. Рижук О. М. Інформаційна безпека України в умовах глобалізаційних викликів та гібридної війни : монографія / за ред. Бебика В. М. ; Відкр. міжнар. ун-т розвитку людини "Україна". Київ : Університет "Україна", 2019. 177 с.

ДОПОМІЖНА ЛІТЕРАТУРА

1. Виговська О., Бєлоусова Н. Інформаційна складова національної безпеки України : кол. монографія / Ін-т міжнар. відносин, Київ. нац. ун-т ім. Тараса Шевченка, Київ. ун-т ім. Бориса Грінченка. Київ : Київ. ун-т ім. Б. Грінченка, 2017. 166 с.
2. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою: навч. посібник / Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.
3. Кавун С. В., Носов В. В, Манжай О. В. Інформаційна безпека. Навчальний посібник / Харків: Вид. ХНЕУ, 2008. 352 с.
4. Міжнародна інформаційна безпека: теорія і практика : підруч. для студентів ВНЗ, які навчаються за напрямом підгот. "Міжнародні відносини" та "Міжнародна інформація" / Є. Макаренко [та ін.] ; Київ. нац. ун-т ім. Тараса Шевченка, [Ін-т міжнар. відносин]. Київ : Центр вільної преси, 2016. 417 с.
5. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.
6. Ніколаєнко Н. О., Комарчук О. О. Засоби масової комунікації як детермінанти гібридної війни : монографія / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2021. 217 с.

ІНТЕРНЕТ-РЕСУРСИ

www.rada.gov.ua
www.president.gov.ua
www.kmu.gov.ua
www.lib.nau.edu.ua/main/
www.nbuv.gov.ua/

Оцінювання курсу

За повністю виконані завдання студент може отримати визначену кількість балів:

Інструменти і завдання	Кількість балів
Участь в обговоренні	20
Тести	25
Індивідуальні завдання	25
Заліковий тест	30
Разом	**100**

Шкала оцінювання студентів

Сума балів за всі види навчальної діяльності	Оцінка ECTS
90–100	A
82–89	B
74–81	C
64–73	D
60–63	E
35–59	FX
0–34	F

Політика курсу

Плагіат та академічна доброчесність

Під час виконання завдань студент має дотримуватись політики академічної доброчесності. Запозичення мають бути оформлені

сність:	відповідними посиланнями. Списування є забороненим.
Завдання і заняття:	Всі завдання, передбачені програмою курсу мають бути виконані своєчасно і оцінені в спосіб, зазначений вище. Аудиторні заняття мають відвідуватись регулярно. Пропущені заняття (з будь-яких причин) мають бути відпрацьовані з отриманням відповідної оцінки не пізніше останнього тижня поточного семестру. В разі поважної причини (хвороба, академічна мобільність тощо) терміни можуть бути збільшені за письмовим дозволом декана. Студент може пройти певні онлайн-курси, які пов'язані з темами дисципліни, на онлайн-платформах. При поданні документу про проходження курсу студенту можуть бути зараховані певні теми курсу та нараховані бали за завдання.
Поведінка в аудиторії:	На заняття студенти вчасно приходять до аудиторії відповідно до діючого розкладу та обов’язково мають дотримуватися вимог техніки безпеки. Під час занять студенти: – не вживають їжу та жувальну гумку; – не залишають аудиторію без дозволу викладача; – не заважають викладачу проводити заняття. Під час контролю знань студенти: – є підготовленими відповідно до вимог даного курсу; – розраховують тільки на власні знання (не шукають інші джерела інформації або «допомоги» інших осіб); – не заважають іншим; – виконують усі вимоги викладачів щодо контролю знань.