Міністерство освіти і науки України

Східноєвропейський національний університет імені Лесі Українки

Кафедра міжнародних комунікацій та політичного аналізу

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної і
навчальної роботи та рекрутації
проф. Гавриліюк С. В. _____
Протокол № 2 від 17.10. 2018 р.

ПРОГРАМА

нормативної навчальної дисципліни

ІНФОРМАЦІЙНА ПОЛІТИКА ТА БЕЗПЕКА

підготовки магістра

галузі знань 06 «Журналістика»

спеціальності 061 «Журналістика»

освітньої програми «Журналістика і соціальні комунікації»

Луцьк –2018

Програма навчальної дисципліни «Інформаційна політика та безпека» для студентів спеціальності 061 «Журналістика» освітньої програми «Журналістика і соціальні комунікації».

Розробник*:* Федонюк С. В.
кандидат географічних наук,
доцент кафедри міжнародних комунікацій та політичного аналізу
Східноєвропейського національного університету імені Лесі Українки

Рецензент:
Доктор політичних наук,
професор кафедри і міжнародних комунікацій
і політичного аналізу Н. П. Карпчук

Програма навчальної дисципліни затверджена
на засіданні кафедри
міжнародних комунікацій та політичного аналізу,
протокол № ___ від ___ .___. 2018 р.

Завідувач кафедри А. М. Митко

Робоча програма навчальної дисципліни схвалена науково-методичною
комісією факультету міжнародних відносин
протокол № від _____ 2018 р.

Голова методичної комісії Романюк Н.І.

Робоча програма навчальної дисципліни схвалена науково-методичною
радою Східноєвропейського національного університету імені Лесі Українки

1. Опис навчальної дисципліни

Таблиця 1

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітня програма</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td rowspan="2">Денна форма навчання</td><td>06
Журналістика</td><td rowspan="2">Нормативна</td></tr>
<tr><td>061 «Журналістика»</td></tr>
<tr><td rowspan="2">Кількість годин / кредитів - 120 / 4</td><td rowspan="5">Журналістика і соціальні комунікації</td><td>Рік підготовки - другий</td></tr>
<tr><td>Семестр - третій</td></tr>
<tr><td rowspan="2">ІНДЗ – немає</td><td>Лекції - 24 год.</td></tr>
<tr><td>Семінарські заняття - 12 год.</td></tr>
<tr><td>Самостійна робота - 76 год</td></tr>
<tr><td></td><td>Консультації – 8 год.</td></tr>
<tr><td></td><td></td><td>Форма контролю - екзамен</td></tr>
</table>

2. Анотація курсу

Дисципліна призначена для знайомства в з політологічними підходами і сучасними тенденціями в оцінці значення проблеми інформаційної безпеки в політичному процесі. Актуальність проблематики зумовлена зростанням впливу інформації на політичні, економічні, військові, культурні процеси розвитку суспільства, а також її недостатньою захищеністю як на зовнішньополітичній арені, так і в Україні.

Основною метою є формування у студентів уявлення про місце проблеми інформаційної безпеки в сучасній політиці, зокрема про:

- генезис розвитку проблеми інформаційної безпеки, як складовій частині загальнополітичного процесу, зміни структури безпеки відповідно до етапів соціо-економічного розвитку;
- існуючі можливості створення й застосування інформаційних засобів дії;
- особливості побудови систем інформаційної безпеки у зв'язку з появою в арсеналах армій різних держав інформаційних засобів дії;
- шляхи формування нової системи глобальної безпеки, події та чинники що впливають на цей процес.

Завдання:

- отримання студентами знань про основні складові забезпечення інформаційної безпеки України в умовах сучасних міжнародних відносин;
- вивчення нормативної бази;
- знайомство з формами і методами створення інформаційної безпеки на міжнародному рівні, в зарубіжних країнах, в Україні.

Результатом є отримання студентами навичок (компетенцій), достатніх для проведення самостійної аналітичної роботи в областях політологічної діяльності, що вимагають співвідношення предмету досліджень з тенденціями в політичному процесі, особливостями і закономірностями соціально-технічних процесів інформаційного суспільства. Формування таких компетенцій у студентів визначається завданням підготовки фахівців, орієнтованих на роботу як в ЗМІ, органах виконавчої влади, інших державних і недержавних відомствах, міжнародних і

громадських організаціях, підрозділах бізнес-компаній, освітніх установах вищої школи діяльність яких пов'язана з аналізом і врахуванням специфіки поточного політичного процесу, прогнозуванням політичних ситуацій, врахуванням питань інформаційної безпеки.

3. Компетенції

ЗНАННЯ Й РОЗУМІННЯ	
Знання і розуміння: • розуміти місце інформаційної безпеки в політичному процесі сучасного світу; • розуміти логіку зміни і розвитку проблеми інформаційної безпеки в історії людства. • розуміти основні процеси, пов'язані із загальною інформатизацією суспільства; • співвідносити глобалізаційні процеси й процеси інформатизації; • розуміти, які засоби дії відносяться до інформаційних і співвідносити ці засоби за їх потенціалом із зброєю масового ураження; • визначати новий характер загроз, пов'язаних із процесом інформатизації, засобів боротьби з ними; • аналізувати основні концептуальні підходи до проблеми забезпечення інформаційної безпеки; • аналізувати конкретні події у сфері військово-політичної безпеки у зв'язку із зміною військових доктрин розвинених країн; • орієнтуватися в проблематиці, що стосується проблеми озброєнь і контролю над ними в новому вимірі інформаційного суспільства.	Освітні методики - лекції; - студентські доповіді; - виконання контрольних робіт; - написання аналітичних довідок. Форма перевірки знань: - контрольні роботи; - аналітичні довідки; - доповіді на заняттях; - підсумковий контроль.
КОМПЕТЕНЦІЇ	
Аналітичні компетенції • розуміння місця інформаційної безпеки в системі безпеки різних акторів світової політики і міжнародних відносин; • знання і розуміння основних аспектів безпеки постіндустріального (інформаційного) суспільства, виділення інформаційної складової безпеки держави, суспільства і особи; • знання суті і форм прояву нових викликів і загроз безпеки в інформаційній сфері; • розуміння ступеня реальності інформаційних загроз для світової спільноти, держав, суспільних груп, виробничих об'єктів; • знання основних методів протидії новим викликам і загрозам в інформаційній сфері на національному і міжнародному рівні; • уміння співвідносити старі загрози безпеки індустріального суспільства із знов виникаючими	Освітні методики (форми проведення занять): - лекції; - підготовка доповідей студентами; - виконання контрольних робіт; - написання аналітичних довідок (індивідуальні науково-дослідні завдання); - аналіз книг і статей з рекомендованої літератури, що відображає високий рівень аналітичних компетенцій; - обговорення матеріалів ЗМІ з актуальних проблем сучасної світової політики. Форма перевірки розвитку (ступеня оволодіння) компетенції: - перевірка в ході занять засвоєння знань і розумінь, одержаних на лекціях і при самостійній роботі;

інформаційними загрозами, а також розставляти пріоритети в боротьбі з ними; • уміння виділяти пріоритетні напрями в питаннях інформаційної безпеки; • здатність розрізняти діяльність із забезпечення інформаційної безпеки різних акторів світової політики і міжнародних відносин; • знання основних напрямів діяльності України у сфері забезпечення національної й міжнародної інформаційної безпеки; • орієнтуватися в позиціях різних країн світу з питань побудови міжнародної системи інформаційної безпеки.	- оцінка й обговорення результатів контрольних робіт; - консультації в процесі написання ІНДЗ та їх оцінка; - підсумкове випробування (залік).
Системні компетенції: - застосування знань з інших дисциплін загальноосвітнього, історичного, економічного, правового й спеціального циклів, а також знання іноземних мов для комплексного аналізу проблем світової політики.	Освітні методики: - демонстрація в ході занять плідності комплексного міждисциплінарного аналізу конкретних проблем світової політики, використовування матеріалів іноземними мовами. Форма перевірки розвитку (ступеня оволодіння) компетенції: - оцінка виступів на семінарах, контрольних і дослідницьких робіт з урахуванням застосування міждисциплінарних знань.
Комунікаційні компетенції - уміння ясно, з використанням прийнятої термінології висловлювати свої думки письмово й усно українською мовою; - уміння пошуку інформації та її оцінки.	Освітні методики (форми проведення занять) – демонстрація високих рівнів письмових комунікаційних компетенцій на прикладі рекомендованої літератури; - детальний розбір усних повідомлень, письмових контрольних робіт, а також аналітичних робіт в аспекті цих комунікаційних компетенцій; Форма перевірки розвитку (ступеня оволодіння) компетенції: -обговорення і оцінка комунікаційних компетенцій в ході усних виступів, контрольних і аналітичних робіт.

4. Інформаційний обсяг навчальної дисципліни

1. Загальні підстави інформаційної політики і безпеки

Інформаційна політика.

Концепція зовнішньої політики і національної безпеки України. Захист єдиного інформаційного простору країни, прав і інтересів держави щодо його формування і збереження.

Доктрина інформаційної безпеки України.

Основні засади інформаційної безпеки України. Інформаційна безпека в системі забезпечення національної безпеки України. Напрями державної політики у сфері інформаційної безпеки України.

Загрози інформаційній безпеці України. Види і джерела загрози безпеки України й інших країн в інформаційній сфері. Два аспекти інформаційної безпеки: інформаційно-технічний і інформаційно-психологічний.

Основні чинники розвитку інформаційної безпеки. Політика і методи використання досягнень НТР в інформаційній сфері. Технічні, технологічні і правові проблеми становлення інформаційної безпеки.

Соціально-психологічні, організаційні і юридичні аспекти інформаційної безпеки.

Концептуальна модель інформаційної безпеки. Напрями, задачі і методи забезпечення інформаційної безпеки в Україні і в інших країнах (порівняльний аналіз) у області зовнішньої і внутрішньої політики, в різних сферах суспільного життя: у сфері економіки, науки і техніка, в оборонній системі, в духовному житті, в інформаційній системі і т.д.

2. Інформаційне протиборство і безпека

Основи протиборства в інформаційній сфері. Типізація активних дій в інформаційному просторі, напряму дії на інформаційні структури.

Нові об'єкти безпеки в інформаційній сфері (відкриті інформаційні мережі, бізнес, суспільна свідомість, інтереси особи).

Інформаційний (кібер-) тероризм і трансформація міжнародного тероризму. Використання кіберпростору в злочинних цілях.

Інформаційна зброя – новий вид зброї масового ураження. Типізація інформаційної зброї.

Інтереси в інформаційному протиборстві.

Загрози міжнародної інформаційної безпеки (МІБ). Принципи класифікації і джерела загроз МІБ. Об'єкти МІБ. Суб'єкти інформаційної дії.

3. Основні національні інтереси України в інформаційній сфері

Основні складові національних інтересів України у сфері інформації й комунікації: дотримання конституційних прав і свобод людини і громадянина в області отримання інформації і користування нею; інформаційне забезпечення державної політики України, призначене для української й зарубіжної громадськості; розвиток сучасних інформаційних технологій, вітчизняної індустрії інформації і комунікацій; захист інформаційних ресурсів, забезпечення безпеки інформаційних і телекомунікаційних систем; розвиток міжнародної співпраці в області інформації, участь у виробленні міжнародно-правових норм цієї співпраці, розширення обміну інформацією.

Визначення і класифікація основних складових інформаційної безпеки на міжнародному рівні, в розвинених зарубіжних країнах, в Україні.

4. Безпека інформаційних систем

Основні поняття безпеки інформаційних технологій. Суб'єкти інформаційних відносин, їх інтереси і безпеку, шляхи нанесення їм шкоди. Основні терміни і визначення. Конфіденційність, цілісність, доступність. Вимоги до інформаційної безпеки (ІБ). Система управління інформаційною безпекою (СУІБ). Концептуальна модель ІБ. Загальна структура засоби забезпечення ІБ. Види оброблюваної інформації. Об'єктно-орієнтований підхід до ІБ. Об'єкти, цілі та завдання захисту інформаційних систем.

Загрози інформаційній безпеці. Класифікація. Основні джерела і шляхи реалізації загроз. Моделі порушників. Підходи до аналізу та управління ризиками, до категорування ресурсів та визначенню вимог до рівня забезпечення інформаційної безпеки. Українські та міжнародні стандарти і критерії захищеності систем.

Заходи забезпечення інформаційної безпеки. Типологія. Основні принципи побудови систем захисту. Принципи парирування загроз.

Основні захисні механізми. Заходи щодо забезпечення ІБ.

Основні помилки при побудові захищених інформаційних систем.

5. Правові основи забезпечення інформаційної безпеки

Закони України та інші нормативно-правові документи, що регламентують відносини суб'єктів в інформаційній сфері та діяльність організацій по захисту інформації. Захист інформації обмеженого доступу, права та обов'язки суб'єктів. Ліцензування діяльності, сертифікація засобів захисту та атестація інформаційних систем. Вимоги керівних документів НБУ, ГССіЗІ і ДСТСЗІ СБУ. Питання законності застосування засобів криптографічного захисту інформації.

Вимоги з безпеки з урахуванням міжнародних стандартів:

ISO / IEC 27000:2009 Визначення і основні принципи. Перша уніфікація з стандартами COBIT і ITIL.

ISO / IEC 27001:2005 Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги. (Раніше BS 7799-2:2005)

ISO / IEC 27002:2005 Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою (раніше ISO / IEC 17799:2005).

ISO / IEC 27003:2007 Інформаційні технології. Методи забезпечення безпеки. Керівництво по впровадженню системи управління інформаційною безпекою.

ISO / IEC 27004:2007 Інформаційні технології. Методи забезпечення безпеки. Вимірювання ефективності системи управління інформаційною безпекою.

ISO / IEC 27005:2007 Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки (на основі BS 7799-3:2006).

ISO / IEC 27006:2007 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікації систем управління інформаційною безпекою.

ISO / IEC 27007 Керівництво для аудитора СУІБ (Draft).

ISO / IEC 27011:2008 Керівництво з управління інформаційною безпекою для телекомунікацій.

Стандарт безпеки даних індустрії платіжних карт (PCI DSS) v.2.0

ISO / IEC 38500:2008 Корпоративний менеджмент інформаційними технологіями;

ДСТУ ISO / IEC TR 13335-1:2003 Технології інформаційні. Рекомендації з управління безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки в ІТ;

ДСТУ ISO / IEC TR 13335-2:2003 Технології інформаційні. Рекомендації з управління безпекою інформаційних технологій. Частина 2. Управління та планування безпеки ІТ;

ДСТУ ISO / IEC TR 13335-5:2005 Технології інформаційні. Рекомендації з управління безпекою інформаційних технологій. Частина 5. Рекомендації щодо управління мережевою безпекою

6. Організація заходів та методів захисту інформації

Оцінка і обробка ризику, Процес оцінки ризиків. Процес обробки ризиків. Компоненти процесу. Встановлення стану. Процес оцінки ризику інформаційний безпеки. Аналіз ризику інформаційної безпеки. Оцінка ризику інформаційної безпеки. Обробка ризику інформаційної безпеки. Прийняття ризику інформаційної безпеки. Ризик інформаційної безпеки системи зв'язку. Ризик інформаційної безпеки моніторингу та перегляду. Підходи в оцінці ризиків інформаційної безпеки.

Політика безпеки. Організація інформаційної безпеки. Внутрішня організація. Забезпечення безпеки за наявності доступу до інформаційних систем сторонніх організацій. Управління активами. Відповідальність за активи. Класифікація інформації.

Питання безпеки, пов'язані з кадровими ресурсами. Перед працевлаштуванням. Під час роботи за трудовою угодою. Припинення дії трудової угоди або його зміна.

Фізичний захист і захист від впливів навколишнього середовища. Охоронювані зони. Безпека обладнання.

Управління засобами зв'язку та операціями. Процедури експлуатації і обов'язки ... Управління постачанням послуг третьою стороною. Планування навантаження і приймання систем. Захист від шкідливого і мобільного коду. Дублювання. Управління безпекою мереж. Маніпулювання носіями інформації. Обмін інформацією. Сервіси електронної торгівлі. Моніторинг.

Контроль доступу. Вимога бізнесу щодо забезпечення контролю доступу. Управління доступом користувача. Обов'язки користувача. Контроль мережевого доступу. Контроль доступу до операційної системи. Контроль доступу до програм та інформації. Моніторинг доступу та використання системи ...

Придбання, удосконалення та обслуговування інформаційних систем. Вимоги безпеки інформаційних систем. Правильна обробка додатків. Криптографічні засоби. Безпека системних файлів. Безпека у процесах розробки і підтримки. Управління технічними вразливостями.

Управління інцидентами порушення інформаційної безпеки. Повідомлення про порушення і слабких місцях інформаційної безпеки. Управління інцидентами порушення інформаційної безпеки та їх удосконалення.

Управління безперервністю бізнесу Аспекти інформаційної безпеки управління безперервністю бізнесу.

Відповідність вимогам. Відповідність правовим вимогам. Відповідність політикам та стандартам безпеки. Технічна відповідність. Питання для розгляду при аудиті інформаційних систем.

7. Система управління ІБ. Вимоги до СУІБ

Загальні вимоги Створення і управління СУІБ. Вимоги до документації. Зобов'язання керівництва Управління ресурсами. Внутрішні аудити СУІБ. Аналіз СУІБ керівництвом Загальні положення. Вхідні дані аналізу. Вихідні дані аналізування.

Удосконалення СУІБ. Безперервне вдосконалення. Коригувальні дії. Превентивні дії.

8. Забезпечення безпеки автоматизованих систем

Проблеми забезпечення безпеки в мережах. Типова IP-мережа організації. Мережеві загрози, вразливості і атаки. Засоби виявлення вразливостей вузлів IP-мереж і атак на вузли, протоколи та мережеві служби. Отримання оперативної інформації про нові вразливості і атаках. Способи усунення вразливостей і протидії вторгненням порушників.

Міжмережеві екрани. Призначення і види. Основні можливості і варіанти розміщення. Переваги і недоліки. Основні захисні механізми: фільтрація пакетів, трансляція мережевих адрес, проміжна аутентифікація, перевірка пошти, віртуальні приватні мережі, протидія атакам, націленим на порушення працездатності мережевих служб, додаткові функції. Загальні рекомендації щодо застосування. Політика безпеки при доступі до мережі загального користування.

Контроль інформаційного наповнення (контенту) електронної пошти та Web-трафіку. Компоненти і функціонування систем контролю контента. Політики безпеки, сценарії та варіанти застосування та реагування.

Віртуальні приватні мережі (VPN). Призначення, основні можливості, принципи функціонування та варіанти реалізації. Структура захищеної корпоративної мережі. Варіанти, достоїнства і недоліки VPN-рішень. Загальні рекомендації щодо їх застосування.

Засоби виявлення вразливостей вузлів мереж і засоби виявлення атак на вузли, протоколи та мережеві служби. Призначення, можливості, принципи роботи. Місце і роль в загальній системі забезпечення безпеки. Порівняння можливостей з міжмережевим екранами. Засоби забезпечення адаптивної мережевої безпеки. Варіанти рішень по забезпеченню безпеки мережі організації.

Структура навчальної дисципліни

Таблиця 2

Назви змістових модулів і тем	Кількість годин				
	Усього	у тому числі			
		Лк.	Пр.	Інд.	Сам.
Тема 1. Загальні підстави інформаційної політики і безпеки	16	4	2		10
Тема 2. Інформаційне протиборство і безпека	16	4	2		10
Тема 3. Основні національні інтереси України в інформаційній сфері	12	4		2	6
Тема 4. Безпека інформаційних систем	14	2		2	10
Тема 5. Правові основи забезпечення інформаційної безпеки	14	2	2		10
Тема 6. Організація заходів та методів захисту інформації	20	4	4	2	10
Тема 7. Система управління ІБ. Вимоги до СУІБ	14	2		2	10
Тема 8. Забезпечення безпеки автоматизованих систем	14	2	2		10
Усього годин	120	24	12	8	76

Теми семінарських занять

№ з/п	Тема	К-сть годин
1	Тема 1. Загальні підстави інформаційної політики і безпеки *Питання для обговорення :* Концепція зовнішньої політики і національної безпеки України. Доктрина інформаційної безпеки України. Загрози інформаційній безпеці України. Основні чинники розвитку інформаційної безпеки.	2
2	Тема 2. Інформаційне протиборство і безпека *Питання для обговорення :* Основи протиборства в інформаційній сфері. Інформаційний (кібер-) тероризм і трансформація міжнародного тероризму. Інформаційна зброя. Інтереси в інформаційному протиборстві. Загрози міжнародної інформаційної безпеки (МІБ). Принципи класифікації і джерела загроз МІБ. Об'єкти МІБ. Суб'єкти інформаційної дії.	2
3	Тема 5. Правові основи забезпечення інформаційної безпеки *Питання для обговорення :* Закони України та інші нормативно-правові документи, що регламентують відносини суб'єктів в інформаційній сфері та діяльність організацій по захисту інформації. Захист інформації обмеженого доступу, права та обов'язки суб'єктів. Ліцензування діяльності, сертифікація засобів захисту та атестація інформаційних систем. Вимоги керівних документів НБУ, ГССіЗІ і ДСТСЗІ СБУ. Вимоги з безпеки з урахуванням міжнародних стандартів	2
4	Тема 6. Організація заходів та методів захисту інформації *Питання для обговорення :* Політика безпеки. Питання безпеки, пов'язані з кадровими ресурсами. Управління засобами зв'язку та операціями.	4

	Контроль доступу. Вимоги безпеки інформаційних систем Управління інцидентами порушення інформаційної безпеки.	
5	Тема 8. Система управління ІБ. Вимоги до СУІБ *Питання для обговорення* Проблеми забезпечення безпеки в мережах. Способи усунення вразливостей і протидії вторгненням порушників. Міжмережеві екрани. Політика безпеки при доступі до мережі загального користування. Віртуальні приватні мережі (VPN).	2
	Разом	12

Самостійна робота

№ з/п	Тема	Кількість годин
1	Загальні підстави інформаційної політики і безпеки	10
2	Інформаційне протиборство і безпека	10
3	Основні національні інтереси України в інформаційній сфері	6
4	Безпека інформаційних систем	10
5	Правові основи забезпечення інформаційної безпеки	10
6	Організація заходів та методів захисту інформації	10
7	Система управління ІБ. Вимоги до СУІБ	10
8	Забезпечення безпеки автоматизованих систем	10
	Разом	76

5. Завдання для індивідуального опрацювання

1. Місце проблеми забезпечення інформаційної безпеки в сучасній світовій політиці.
2. Поняття «безпеки» в інформаційному суспільстві.
3. Теоретичні підходи до аналізу логіки інформаційної війни і забезпечення військово-політичної безпеки.
4. Основні чинники, що визначають нові параметри проблеми забезпечення інформаційної безпеки.
5. Зміна характеру і пріоритетності загроз міжнародної інформаційної безпеки.
6. Співвідношення завдань забезпечення національної і міжнародної інформаційної безпеки.
7. Проблема міжнародного інформаційного тероризму.
8. Зміна парадигм тероризму в інформаційному суспільстві.
9. Проблема правового регулювання конфліктів із застосуванням інформаційних засобів дії.
10. Проблема війни і миру в інформаційному суспільстві.
11. Аналіз одного з сучасних конфліктів із позицій інформаційного протиборства.
12. Проблема розповсюдження інформаційної зброї.
13. Проблема контролю над інформаційними озброєннями.
14. Зміна характеру і пріоритетності загроз безпеки в інформаційному суспільстві.
15. Співпраця і розбіжності в підходах у сфері забезпечення міжнародної інформаційної безпеки між РФ і США.

6. Розподіл балів та критерії оцінювання

Таблиця 3

Поточний контроль (мах = 40 балів)						**Модульний контроль (мах = 60 балів)**	**Загальна кількість балів**
Модуль 1					**ІНДЗ**	**Модуль 3**	
						МКР	
С1	С2	С3	С4	С5	10	60	100
6	6	6	6	6			

Робота студента на семінарських заняттях за кожною темою програми оцінюється максимально у 6 балів, в тім: виступ – до 4 балів (розширений виступ із дискусією – 4, доповідь – 2, повідомлення – 2 бали); участь у дискусії – 2 бали; підготовка матеріалу до виступу (конспект) – 2 бали.

Студент отримує позитивну оцінку, якщо він повністю виконав навчальну програму з дисципліни, атестований за результатами модулів, набрав відповідну кількість балів за роботу на семінарських заняттях, самостійну та індивідуальну роботу, успішно склав екзамен і в сумі отримав не менше 60 балів.

Підсумковий контроль проходить у формі екзамену (обов'язковий), за складання якого студент може отримати максимум 60 балів.

Під час підсумкового контролю студент отримує:

– 50-60 балів, якщо він дає повну, вичерпну відповідь на поставлені запитання, вільно використовуючи поняття й терміни, що передбачені до вивчення цією програмою, успішно вирішує ситуаційні завдання, наводить власні приклади, дає правильну відповідь на поставлені додаткові завдання, застосовуючи при цьому знання, здобуті при вивченні інших навчальних дисциплін, що передбачені програмою підготовки магістра;

– 38-49 бали, якщо відповідь студента на всі запитання є повною, але загалом має репродуктивний характер і містить незначну кількість несуттєвих недоліків;

– 26-37 балів, якщо відповідь загалом повна, але значні недоліки з окремих питань;

– 14-25 балів, якщо відсутня відповідь на окремі запитання;

– 1-13 балів, якщо відповідь на окремі запитання фрагментарна, а на інші – відсутня;

– 0 балів, якщо відповідь відсутня.

Загальна сума балів за курс – 100. Оцінка за освоєння курсу виставляється відповідно до шкали оцінювання (табл. 4).

Таблиця 4

Шкала оцінювання

Сума балів за всі види навчальної діяльності	**Оцінка**
90 – 100	Відмінно
82 – 89	Дуже добре
75 - 81	Добре
67 -74	Задовільно
60 - 66	Достатньо
1 – 59	Незадовільно

7. Рекомендована література

1. Бойченко О. В. Міжнародна інформаційна безпека: проблеми і перспективи / О. В. Бойченко // Форум права. – 2009. – № 3. – С. 74–79 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2009-3/09bovpip.pdf
2. Бойченко О. В. Міжнародне співробітництво правоохоронних органів держав в галузі забезпечення інформаційної безпеки / О. В. Бойченко // Форум права. – 2009. – № 2. – С. 56–62 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2009-2/09bovzou.pdf.
3. Гуз А. М. Історія захисту інформації в Україні в Україні та провідних країнах світу : навчальний посібник [для студ. вищ. навч. закл.] / А. М. Гуз. – К. : КНТ, 2007. – 260 с.
4. Декларация принципов: Построение информационного общества – глобальная задача в новом тысячелетии [Електронний ресурс]. – Документ WSIS-03/GENEVA/DOC/4-R. 12 декабря 2003 года. – Режим доступу: http://www.itu.int/wsis.
5. План действий [Електронний ресурс]. – Документ WSIS-03/GENEVA/DOC/5-R. 12 декабря 2003 года. – Режим доступу: http://www.itu.int/wsis.
6. Підсумкові документи Всесвітнього самміту з питань інформаційного суспільства / Міністерство транспорту та зв'язку України, Державний Департамент з питань зв'язку та інформатизації. – К., 2006. – 77 с.
7. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: Навч. Посібник / Б. А. Кормич. – К. : Кондор, 2004. – 384 с.
8. Крутских А. В, Федоров А. В. О международной информационной безопасности / А.В. Крутских, А. В. Федоров // Международная жизнь, 2000, № 2.
9. Лопатин В. Н. Правовые основы информационной безопасности / В. Н. Лопатин. - М. : МИФИ, 2000.
10. Макаренко Є. А. Політичні доктрини глобальної інформаційної безпеки / Є. А. Макаренко // Вісник Ін-ту міжнародних відносин Київськ. нац. ун-ту імені Тараса Шевченка. – 2007. – № 2. – С. 45-51.
11. Указ Президента України «Про Доктрину інформаційної безпеки України» : від 08.07.2009 р., № 514/2009 // Офіційний вісник України. – 2009. – №5 2. – Ст. 1783.
12. Федоров А. В., Цыгичко В. Н. (ред.). Информационные вызовы национальной и международной безопасности / А. В. Федоров, В. Н. Цыгичко. - М. : Пир-центр, 2001.
13. Федоров А. В. Информационная безопасность в мировом политическом процессе / А. В. Федоров. - М. : МГИМО (У). 2006.
14. Федоров А. В. Информационная безопасность в международных отношениях, политике и праве зарубежных стран / А. В. Федоров. - М. : МГИМО (У). 2008.

15. Методи та засоби навчання

16. Методи навчання: інформаційно-рецептивний; ілюстративний; репродуктивний; метод проблемного викладу; евристичний.

17.

18. Форма підсумкового контролю успішності навчання

19. Формою підсумкового контролю є екзамен.

20.

21. Методи та засоби діагностики успішності

22. Діагностика знань студентів під час навчального процесу здійснюється з допомогою:

23. 1) усних опитувань на семінарських заняттях;

24. 2) письмових модульних контрольних робіт.