НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
Факультет соціології і права

ЗАТВЕРДЖУЮ
Декан ФСП
_____ Мельниченко А.А.
(підпис)
«____»_____ 2015 р.

_____ _____
(підпис) (ініціали, прізвище)
«____»_____ 20__ р.

ПУБЛІЧНО-ПРАВОВА ОХОРОНА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (ВП – 01/в)

РОБОЧА ПРОГРАМА
кредитного модуля

підготовки **студентів освітнього рівня магістр**
напряму **6.030401 «Правознавство»**
спеціальності **8.03040101 «Правознавство»**
спеціалізації **Інформаційне право**
форми навчання **денна**

Ухвалено методичною комісією
факультету соціології і права
Протокол від ____2015 р. № ___
Голова методичної комісії

_____ _____
(підпис)

«____»_____ 2015 р.

Київ – 2015

Робоча програма кредитного модуля «Публічно-правова охорона інформаційної безпеки» для студентів за напрямом підготовки 6.030401 «Правознавство», спеціальності 8.03040101 «Правознавство», освітнього ступеня магістра за денною формою навчання складена відповідно до програми навчальної дисципліни «Публічно-правова охорона інформаційної безпеки».

Розробники робочої програми:

професор кафедри публічного права,
доктор юридичних наук, професор Мисливий В. А. _____
(підпис)

доцент кафедри публічного права,
кандидат юридичних наук, Попов К. Л. _____
(підпис)

Програму затверджено на засіданні кафедри публічного права

Протокол від «____»_____2015 року № ___

Завідувач кафедри
_____ Чепульченко Т.О.
(підпис)

«___»_____2015 р.

© НТУУ «КПІ», 2015 рік

1. Опис кредитного модуля

<table>
<tr><th>Галузь знань, напрям підготовки, спеціальність, освітній ступінь</th><th>Загальні показники</th><th>Характеристика кредитного модуля</th></tr>
<tr><td>Галузь знань
0304 «Право»</td><td>Назва дисципліни,
до якої належить кредитний модуль
«Публічно-правова охорона інформаційної безпеки»</td><td>Форма навчання
денна</td></tr>
<tr><td>Напрям підготовки
6.030401
«Правознавство»</td><td>Кількість
кредитів ECTS
3</td><td>Статус кредитного модуля
за вибором студента</td></tr>
<tr><td>Спеціальність
8.03040101
«Правознавство»</td><td>Кількість
розділів
3</td><td>Цикл до якого належить кредитний модуль
Професійно-практичної підготовки</td></tr>
<tr><td rowspan="2">Спеціалізація
Інформаційне право</td><td rowspan="2">Індивідуальне завдання
реферат</td><td>Рік підготовки 1</td></tr>
<tr><td>Семестр 1</td></tr>
<tr><td rowspan="4">Освітній ступінь
магістр</td><td rowspan="3">Загальна кількість годин
90</td><td>Лекції
18 год.</td></tr>
<tr><td>Семінарські
18 год.</td></tr>
<tr><td>Лабораторні (комп’ютерний практикум)
не передбачено</td></tr>
<tr><td rowspan="2">Тижневих годин:
аудиторних – 2
СРС – 3</td><td>Самостійна робота
54 год.,
у тому числі на виконання індивідуального завдання
6 год.</td></tr>
<tr><td>Вид та форма семестрового контролю
диф. залік</td></tr>
</table>

В умовах зростання інформаційної насиченості суспільного життя, інтенсивної інформатизації економічної, соціальної, політичної та інших сфер життєдіяльності нашої держави актуалізується необхідність правового забезпечення охорони інформаційних відносин від протиправних посягань. Кількість правопорушень у сфері інформаційних відносин постійно зростає, а

тому протидія ним постає одним з важливих завдань держави, виконання якого потребує належного публічно-правового забезпечення. Завдяки вивченню, опануванню та вдосконаленню відповідного національного законодавства, наближенню його до високих правових стандартів, належному застосуванню правових приписів можна забезпечити належний рівень інформаційної безпеки в Україні.

Вивчення кредитного модуля ВП-01/в «Публічно-правова охорона інформаційної безпеки» має важливе теоретичне і практичне значення у підготовці юристів. Підвищуючи рівень спеціалізованих правових знань студентів як майбутніх спеціалістів з правового регулювання інформаційних відносин, а також формуючи у студентів відповідні навички правозастосування, викладання кредитного модуля ВП-01/в «Публічно-правова охорона інформаційної безпеки» сприятиме формуванню ефективної інформаційно-правової політики в Україні на міцній науковій основі та з належним рівнем професіоналізму.

Засвоєння матеріалу кредитного модуля студентами-правниками є не лише необхідною умовою якісного здійснення ними в майбутньому фахових завдань юриста, але й дозволить значно підвищити рівень професійної спеціалізації у сфері правового регулювання інформаційних відносин.

Кредитний модуль ВП-01/в «Публічно-правова охорона інформаційної безпеки» є складовою частиною блоку навчальних дисциплін спеціалізації «Інформаційне право» циклу професійної та практичної підготовки.

Кредитний модуль ВП-01/в «Публічно-правова охорона інформаційної безпеки» органічно пов'язаний з кредитними модулями НП-12/1 «Кримінальне право (загальна частина) – 1», НП-12/2 «Кримінальне право (загальна частина) – 2», НП-12/3 «Кримінальне право (особлива частина) – 1», НП-12/4 «Кримінальне право (особлива частина) – 2» дисципліни «Кримінальне право», кредитними модулями дисциплін «Конституційне право», «Адміністративне право», «Міжнародне право», які є основою для його вивчення і мають викладатися перед ним за часом.

Кредитний модуль ВП-01/в «Публічно-правова охорона інформаційної безпеки» знаходиться у тісному зв`язку з кредитними модулями дисциплін кримінально-правового циклу («Кримінологія», «Криміналістика»), використовуючи систему знань, які є змістом цих дисциплін.

Кредитний модуль ВП-01/в «Публічно-правова охорона інформаційної безпеки» як складова блоку навчальних дисциплін спеціалізації «Інформаційне право» циклу професійної та практичної підготовки перебуває у тісному зв'язку з іншими дисциплінами цієї спеціалізації («Інформаційне право», «Міжнародне інформаційне право», «Інформаційні ресурси», «Основи інформаційної безпеки»), базуючись на знаннях, одержаних студентом під час їх вивчення. Кредитний модуль ВП-01/в «Публічно-правова охорона інформаційної безпеки» перебуває у певному зв'язку з дисциплінами циклу гуманітарної та соціально-економічної підготовки студентів-правників. Такими дисциплінами, зокрема, є історія, філософія, логіка, економічна теорія, психологія, соціологія та ін. Ці галузі знань створюють загальну світоглядну і методологічну основу

для сприйняття студентами змісту навчальної дисципліни «Публічно-правова охорона інформаційної безпеки».

2. Мета та завдання кредитного модуля

2.1. Метою кредитного модуля є формування у студентів здатностей:

– орієнтуватися у нормах міжнародного права, які забезпечують інформаційну безпеку, здійснювати їх системне тлумачення і правильне застосування;

– застосовувати у професійній діяльності кримінально-правові норми для правильної правової оцінки діянь, які посягають на інформаційну безпеку;

– орієнтуватися у нормах адміністративного законодавства, які забезпечують охорону інформаційної безпеки, виявляючи структуру і зміст ознак складу відповідних правопорушень;

– здійснювати творчий пошук шляхів і засобів удосконалення публічно-правової охорони інформаційної безпеки, формувати відповідні моделі і механізми її захисту.

2.2. Основні завдання кредитного модуля

Згідно з вимогами програми навчальної дисципліни студенти після засвоєння кредитного модуля мають продемонструвати такі результати навчання:

знання:

– поняття, структури і змісту інформаційних відносин та інформаційної безпеки як об’єктів публічно-правової охорони;

– поняття, змісту і видів публічно-правової охорони інформаційної безпеки;

– змісту основних міжнародних договорів з питань охорони інформаційної безпеки;

– особливостей кваліфікації злочинів, які посягають на інформаційний ресурс;

– особливостей кваліфікації злочинів, які посягають на порядок доступу до інформації;

– особливостей кваліфікації злочинів, які посягають на інформаційні відносини у сфері використання інформаційних технологій;

– змісту адміністративно-правового забезпечення охорони інформаційного ресурсу та захисту інформації з обмеженим доступом;

– змісту адміністративно-правового забезпечення доступу до інформації;

– змісту адміністративно-правового забезпечення захисту інформації у сфері використання інформаційних технологій.

уміння:

– орієнтуватися в положеннях міжнародного законодавства з питань забезпечення інформаційної безпеки, здійснювати їх системний аналіз та відшукувати необхідні для правової оцінки міжнародно-правові норми;

– орієнтуватися в положеннях кримінального законодавства, які забезпечують інформаційну безпеку, здійснювати їх системний аналіз та відшукувати необхідну для правової оцінки конкретної ситуації кримінально-правову норму (норми);

– орієнтуватися в положеннях адміністративного законодавства з питань інформаційної безпеки, здійснювати їх системний аналіз та відшукувати необхідну для правової оцінки конкретної ситуації адміністративно-правову норму (норми);

– надавати правильну юридичну оцінку правопорушенням у сфері інформаційної безпеки;

– досліджувати юридичну (зокрема, судову) практику у провадженнях, пов'язаних з посяганням на інформаційну безпеку, оцінюючи дотримання законності у процесі правозастосовної діяльності;

– моделювати механізми публічно-правового забезпечення (охорони) інформаційної безпеки.

досвід:

– виявлення правової природи правопорушень у сфері інформаційної безпеки, виявлення структури і змісту ознак відповідних правопорушень;

– правильної кваліфікації правопорушень у сфері інформаційної безпеки;

– виявлення прогалин в законодавстві, яке забезпечує охорону інформаційної безпеки.

3. Структура кредитного модуля

Назви розділів і тем	Кількість годин			
	Всього	у тому числі		
		Лекції	Семінарські	СРС
1	2	3	4	5
Розділ 1. Загальні положення щодо захисту інформації				
Тема 1.1. Інформаційні відносини та інформаційна безпека як об'єкт правової охорони	10	2	2	6
Тема 1.2. Поняття, зміст і види публічно-правової охорони інформаційної безпеки	10	2	2	6
Тема 1.3. Міжнародно-правова охорона інформаційної безпеки	10	2	2	6
Контрольна робота			(1)	
Разом за розділом 1	**30**	**6**	**6**	**18**
Розділ 2. Кримінально-правова охорона (захист) інформаційної безпеки				
Тема 2.1. Кримінально-правова охорона «інформаційного поля» (інформаційного ресурсу)	12	2	2	6
Тема 2.2. Кримінально-правова охорона порядку доступу до інформації	12	2	2	6
Тема 2.3. Кримінально-правова охорона інформаційних відносин у сфері використання інформаційних технологій	12	2	2	6

1	2	3	4	5
Контрольна робота			(1)	
Разом за розділом 2	**30**	**6**	**6**	**18**
Розділ 3. Адміністративно-правове забезпечення захисту інформації				
Тема 3.1. Адміністративно-правове забезпечення охорони інформаційного ресурсу та захисту інформації з обмеженим доступом	12	2	2	6
Тема 3.2. Адміністративно-правове забезпечення доступу до інформації	12	2	2	6
Тема 3.3. Адміністративно-правове забезпечення захисту інформації у сфері використання інформаційних технологій	12	2	2	6
Контрольна робота			(1)	
Разом за розділом 3	**30**	**6**	**6**	**18**
Реферат				**(6)**
Залік				**(6)**
Всього годин	**90**	**18**	**18**	**54**

4. Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань (перелік дидактичних засобів, посилання на літературу та завдання на СРС)
1	**Тема 1.1. Інформаційні відносини та інформаційна безпека як об'єкт правової охорони** Поняття інформаційних відносин та інформаційної безпеки як об'єкта правової охорони. Складові (структура) інформаційних відносин та інформаційної безпеки. Види інформаційних відносин. Інформація як предмет правопорушення. Види інформації. Інформаційна сфера, інформаційне середовище, інформаційна система, «інформаційне поле», інформатизація. Засоби захисту інформації та охорони інформаційних відносин (публічно-правові, приватно-правові, технічні, фізичні тощо). Інформаційна безпека і засоби її правового забезпечення. Інформаційні війни та інформаційний тероризм. **Література:** базова: 1 – 17, допоміжна: 2, 3, 5, 8-10, 14-17, 20, 21, 23, 24, 28, 29, 31, 32. **Завдання на СРС:** 1. Якими є наслідки порушення інформаційних відносин? 2. Якими є складові інформаційної безпеки? 3. У чому специфіка інформації як предмета правопорушення? 4. Яким є співвідношення захисту інформації і охорони інформаційних відносин? 5. Якими засобами забезпечується охорона інформаційних відносин? 6. Що таке інформаційні війни? Загальні засоби і правила ведення інформаційних війн? 7. Інформація як предмет і засіб тероризму.
2	**Тема 1.2. Поняття, зміст і види публічно-правової охорони інформаційної безпеки** Поняття і значення публічно-правової охорони інформаційної безпеки та охорони інформаційних відносин. Нормативно-правове забезпечення

	захисту інформації. Конституційно-правові підстави захисту інформації. Права на інформацію – інформаційні права – право інтелектуальної власності – право власності. Система публічно-правової охорони інформаційної безпеки. Суб'єкти і учасники публічно-правової охорони інформаційної безпеки. Охорона інформаційної безпеки засобами міжнародного, адміністративного, і кримінального права. Юридична відповідальність за порушення законодавства про інформацію. Криміналізація/декриміналізація в інформаційній сфері. Термінологічний апарат міжнародного, адміністративного і кримінального права щодо захисту інформаційної безпеки. Загальна характеристика публічно-правової охорони інформаційної безпеки у зарубіжних країнах. **Література:** базова: 1 – 17, допоміжна: 1, 4, 6, 7, 12, 13, 19, 25, 26, 27, 30. **Завдання на СРС:** 1. Нормативно-правові акти в сфері захисту інформації. 2. Публічно-правова і приватно-правова охорона інформаційних відносин. 3. Інтелектуальна власність та інформація: правове регулювання. 4. Співвідношення засобів міжнародного, адміністративного і кримінально-правового забезпечення інформаційної безпеки. 5. Якими є системи і особливості правової охорони інформаційної безпеки в зарубіжних країнах?
3	**Тема 1.3. Міжнародно-правова охорона інформаційної безпеки** Міжнародні договори з питань охорони інформаційної безпеки. Глобалізація, інтернаціоналізація та інформаційна безпека. Внутрішня, зовнішня і глобальна інформаційна безпека. Законодавство ЄС щодо інформаційної безпеки. Правове забезпечення координації діяльності різних країн із забезпечення інформаційної безпеки. Правова охорона міжнародного (міждержавного) інформаційного обміну. **Література:** базова: 1 – 17, допоміжна: 11, 22. **Завдання на СРС:** 1. Яким є вплив глобалізаційних процесів на інформаційну безпеку? 2. Глобальні загрози міжнародній інформаційній безпеці. 3. У чому полягає зміст європейських стандартів правового забезпечення інформаційної безпеки? 4. Міжнародна координація та міжнародний інформаційний обмін. 5. Інформаційний суверенітет та інтернаціоналізація.
4	**Тема 2.1. Кримінально-правова охорона «інформаційного поля» (інформаційного ресурсу)** Особливості формування інформаційного ресурсу кримінально-правової охорони. Кримінальна відповідальність за публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади. Кримінальна відповідальність за заклики до дій, вчинених з метою зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України. Кримінальна відповідальність за перешкоджання законній професійній діяльності журналістів. Кримінальна відповідальність за публічні заклики до вчинення терористичного акту. Кримінальна відповідальність за ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи

	релігійну нетерпимість та дискримінацію. Кримінальна відповідальність за ввезення, виготовлення, збут і розповсюдження порнографічних предметів. Службове підроблення. **Література:** допоміжна:3, 7, 13, 14, 21, 25. **Завдання на СРС:** 1. Інформаційне поле (ресурс) як об'єкт кримінально-правової охорони. 2. Якими є особливості кваліфікації перешкоджання законній професійній діяльності журналістів? 3. У чому полягає склад злочину, передбачений ст. 300 КК України? 4. Інформаційний тероризм. 5. Підроблення документів та інші посягання на документообіг.
5	**Тема 2.2. Кримінально-правова охорона порядку доступу до інформації** Кримінальна відповідальність за злочини, пов'язані з порушенням порядку охорони державної таємниці та інформації, яка є власністю держави (ст. 111, 114, 328, 329, 330 КК України). Кримінальна відповідальність за незаконне розголошення лікарської таємниці. Кримінальна відповідальність за злочини проти порядку охорони конфіденційної інформації про особу (ст. 163, 168, 182 КК України). Кримінальна відповідальність за незаконні дії з відомостями, які становлять комерційну, банківську таємницю чи інсайдерську інформацію (ст. 231, 232, 232^1 КК України), порушення порядку ведення бази даних про вкладників або порядку формування звітності (ст. 220^1 КК України). Кримінальна відповідальність за розголошення даних досудового слідства та відомостей про заходи безпеки щодо особи, взятої під захист (ст. 381, 387 КК). Завідомо неправдиве показання (ст. 384 КК України). **Література:** допоміжна: 3, 7, 9, 16, 17, 18, 20, 24, 27, 30. **Завдання на СРС:** 1. У чому полягають особливості кримінально-правової охорони державної таємниці? 2. Конфіденційна інформація: питання охорони. 3. У чому полягає склад злочину, передбачений ст. 231, 232, 232^1 КК України? 4. Якими ознаками характеризуються склади злочинів, передбачені ст. 381, 387 КК України?
6	**Тема 2.3. Кримінально-правова охорона інформаційних відносин у сфері використання інформаційних технологій** Кримінальна відповідальність за незаконні дії з інформацією, що міститься у базі даних Державного реєстру виборців (ст. 158 КК України). Кримінальна відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів) (ЕОМ), автоматизованих систем (АС), комп'ютерних мереж (КМ) чи мереж електрозв'язку (МЕ). Кримінальна відповідальність за створення шкідливих програмних чи технічних засобів. Кримінальна відповідальність за несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в ЕОМ, автоматизованих системах, комп'ютерних мережах. Кримінальна відповідальність за несанкціоновані дії з інформацією, яка оброблюється в ЕОМ, АС, КМ. Кримінальна відповідальність за порушення правил експлуатації ЕОМ, АС, КМ. Порушення правил експлуатації ЕОМ, АС, КМ, МЕ. Кримінальна відповідальність за перешкоджання роботі ЕОМ, АС, КМ,

	МЕ шляхом масового розповсюдження повідомлень електрозв'язку. Кримінальна відповідальність за незаконне втручання в роботу автоматизованої системи документообігу суду (ст. 376^1 КК України). **Література:** допоміжна:1, 2, 4-8, 10, 11, 15, 19, 22, 23, 26, 29, 31. **Завдання на СРС:** 1. Якими є особливості кваліфікації несанкціонованого втручання в роботу ЕОМ, АС, КМ чи МЕ? 2. У чому полягає склад створення шкідливих програмних чи технічних засобів? 3. Якими є особливості кваліфікації несанкціонованих дій з інформацією, яка оброблюється в ЕОМ, АС, КМ? 4. Якими ознаками характеризується порушення правил експлуатації ЕОМ, АС, КМ?
7	**Тема 3.1. Адміністративно-правове забезпечення охорони інформаційного ресурсу та захисту інформації з обмеженим доступом** Порушення законодавства про Національний архівний фонд та архівні установи (ст. 92^1 КпАП). Порушення умов і правил, що регламентують діяльність у сфері телекомунікацій та користування радіочастотним ресурсом України, передбачену ліцензіями, дозволами (ст. 145 КпАП). Незаконне використання інсайдерської інформації (ст. 163^9 КпАП). Порушення порядку розкриття інформації на фондовому ринку (ст. 163^{11} КпАП). Незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових повноважень (ст. 172^8 КУпАП). Поширювання неправдивих чуток (ст. 173^1 КпАП). Розголошення відомостей про заходи безпеки щодо особи, взятої під захист (ст. 185^{11} КУпАП). Порушення законодавства у сфері захисту персональних даних (ст. 188^{39} КУпАП). Незаконне зберігання спеціальних технічних засобів негласного отримання інформації (ст. 195^5 КУпАП). Порушення порядку обліку, зберігання і використання документів та інших носіїв інформації, які містять конфіденційну інформацію, що є власністю держави (ст. 212^5 КУпАП). **Література:** допоміжна:1 – 12. **Завдання на СРС:** 1. У чому полягають ознаки адміністративного правопорушення, передбаченого ст. 145 КУпАП? 2. Якими є ознаки юридичних складів правопорушень, які посягають на порядок використання інсайдерської інформації (інформації на фондовому ринку)? 3. У чому полягає склад правопорушення, передбаченого ст. 188^{39} КУпАП? 4. Якими ознаками характеризується юридичний склад порушення порядку обліку, зберігання і використання документів та інших носіїв інформації, які містять конфіденційну інформацію, що є власністю держави (ст. 212^5 КУпАП)? 5. Якими є особливості кваліфікації порушення законодавства у сфері захисту персональних даних (ст. 188^{39} КУпАП)?
8	**Тема 3.2. Адміністративно-правове забезпечення доступу до інформації** Приховування, перекручення або відмова від надання повної та достовірної інформації за запитами посадових осіб і зверненнями громадян та

	їх об'єднань щодо безпеки утворення відходів та поводження з ними (ст. 82^3 КУпАП). Відмова від надання чи несвоєчасне надання екологічної інформації (ст. 91^4 КУпАП). Порушення законодавства про захист прав споживачів (ст. 156^1 КУпАП). Приховування інформації про діяльність емітента (ст. 163^5 КУпАП). Порушення законодавства про державну таємницю (ст. 212^2 КУпАП). Порушення права на інформацію (ст. 212^3 КУпАП) **Література:** допоміжна:1-12. **Завдання на СРС:** 1. Якими є адміністративно-правові засоби забезпечення доступу до інформації? 2. Якими є ознаки складу правопорушення, передбаченого ст. 91^4 КУпАП? 3. У чому полягає порушення законодавства про захист прав споживачів, передбачене ст. 156^1 КУпАП? 4. Якими ознаками характеризується юридичний склад порушення права на інформацію (ст. 212^3 КУпАП)?
9	**Тема 3.3. Адміністративно-правове забезпечення захисту інформації у сфері використання інформаційних технологій** Порушення правил реалізації, експлуатації радіоелектронних засобів та випромінювальних пристроїв, а також користування радіочастотним ресурсом України (ст. 146 КУпАП). Порушення правил охорони ліній і споруд зв'язку (ст. 147 КУпАП). Порушення Правил надання та отримання телекомунікаційних послуг (ст. 148^1 КУпАП). Порушення порядку та умов надання послуг зв'язку в мережах загального користування (ст. 148^2 КУпАП). Порушення правил про взаємоз'єднання телекомунікаційних мереж загального користування (ст. 148^5 КУпАП). Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем (ст. 212^6 КУпАП). **Література:** допоміжна:1-13. **Завдання на СРС:** 1. Якими є ознаки порушення правил реалізації, експлуатації радіоелектронних засобів та випромінювальних пристроїв, а також користування радіочастотним ресурсом України (ст. 146 КУпАП)? 2. Якими є ознаки об’єктивної сторони порушення Правил надання та отримання телекомунікаційних послуг (ст. 148^1 КУпАП)? 3. Якими є ознаки злочину, передбаченого ст. 148^2 КУпАП? 4. Якими ознаками характеризується склад злочину, передбаченого ст. 212^6 КУпАП?

5. Практичні заняття

Не передбачено навчальним планом

6. Семінарські заняття

Основні завдання циклу семінарських занять: сформувати у студентів розуміння сутності правопорушень, які посягають на інформаційну безпеку,

вміння кваліфікувати відповідні правопорушення, виявляючи ознаки їх юридичного складу.

№ з/п	Назва теми заняття та перелік основних питань (перелік дидактичного забезпечення, посилання на літературу та завдання на СРС)
1	**Тема 1.1. Інформаційні відносини та інформаційна безпека як об'єкт правової охорони** 1. Складові (структура) інформаційних відносин та інформаційної безпеки. 2. Інформація як предмет правопорушення. Види інформації. 3. Засоби захисту інформації та охорони інформаційних відносин (публічно-правові, приватно-правові, технічні, фізичні тощо). 4. Інформаційні війни та інформаційний тероризм: загрози і правовий механізм протидії. **Література:** базова: 1 – 17, допоміжна: 2, 3, 5, 8-10, 14-17, 20, 21, 23, 24, 28, 29, 31, 32. **Завдання на СРС:** опрацювання питань, передбачених змістом теми 1.2.
2	**Тема 1.2. Поняття, зміст і види публічно-правової охорони інформаційної безпеки** 1. Поняття і значення публічно-правової охорони інформаційної безпеки та охорони інформаційних відносин. 2. Конституційно-правові підстави захисту інформації. 3. Співвідношення понять: права на інформацію – інформаційні права – право інтелектуальної власності – право власності. 4. Система публічно-правової охорони інформаційної безпеки. 5. Термінологічний апарат міжнародного, адміністративного і кримінального права щодо захисту інформаційної безпеки. **Література:** базова: 1 – 17, допоміжна: 1, 4, 6, 7, 12, 13, 19, 25, 26, 27, 30. **Завдання на СРС:** опрацювання питань, передбачених змістом теми 1.3
3	**Тема 1.3. Міжнародно-правова охорона інформаційної безпеки** 1. Міжнародні договори з питань охорони інформаційної безпеки. 2. Вплив глобалізаційних, інтернаціоналізаційних процесів та інформаційну безпеку. 3. Основні положення законодавства ЄС щодо інформаційної безпеки. 4. Правова охорона міжнародного (міждержавного) інформаційного обміну. **Література:** базова: 1 – 17, допоміжна: 11, 22. **Завдання на СРС:** вирішення задач (визначається викладачем згідно з додатком до робочої програми кредитного модуля).
4	**Тема 2.1. Кримінально-правова охорона «інформаційного поля» (інформаційного ресурсу)** 1. Кримінальна відповідальність за публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади. 2. Кримінальна відповідальність за заклики до дій, вчинених з метою зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України.

	3. Кримінальна відповідальність за перешкоджання законній професійній діяльності журналістів. 4. Кримінальна відповідальність за ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію. 5. Службове підроблення. **Література:** допоміжна:3, 7, 13, 14, 21, 25. **Завдання на СРС:** вирішення задач (визначається викладачем згідно з додатком до робочої програми кредитного модуля).
5	**Тема 2.2. Кримінально-правова охорона порядку доступу до інформації** 1. Кримінальна відповідальність за злочини, пов'язані з порушенням порядку охорони державної таємниці та інформації, яка є власністю держави (ст. 111, 114, 328, 329, 330 КК України). 2. Кримінальна відповідальність за злочини проти порядку охорони конфіденційної інформації про особу (ст. 163, 168, 182 КК України). 3. Кримінальна відповідальність за незаконні дії з відомостями, які становлять комерційну, банківську таємницю чи інсайдерську інформацію (ст. 231, 232, 232^1 КК України). 4. Кримінальна відповідальність за розголошення даних досудового слідства та відомостей про заходи безпеки щодо особи, взятої під захист (ст. 381, 387 КК). **Література:** допоміжна: 3, 7, 9, 16, 17, 18, 20, 24, 27, 30. **Завдання на СРС:** вирішення задач (визначається викладачем згідно з додатком до робочої програми кредитного модуля).
6	**Тема 2.3. Кримінально-правова охорона інформаційних відносин у сфері використання інформаційних технологій** 1. Кримінальна відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. 2. Кримінальна відповідальність за створення шкідливих програмних чи технічних засобів. 3. Кримінальна відповідальність за несанкціоновані дії з інформацією, яка оброблюється в ЕОМ, АС, КМ. 4. Кримінальна відповідальність за порушення правил експлуатації ЕОМ, АС, КМ. Порушення правил експлуатації ЕОМ, АС, КМ, МЕ. 5. Кримінальна відповідальність за перешкоджання роботі ЕОМ, АС, КМ, МЕ шляхом масового розповсюдження повідомлень електрозв'язку. **Література:** допоміжна:1, 2, 4-8, 10, 11, 15, 19, 22, 23, 26, 29, 31. **Завдання на СРС:** вирішення задач (визначається викладачем згідно з додатком до робочої програми кредитного модуля).
7	**Тема 3.1. Адміністративно-правове забезпечення охорони інформаційного ресурсу та захисту інформації з обмеженим доступом** 1. Порушення умов і правил, що регламентують діяльність у сфері телекомунікацій та користування радіочастотним ресурсом України, передбачену ліцензіями, дозволами (ст. 145 КУпАП). 2. Незаконне використання інсайдерської інформації (ст. 163^9 КУпАП). Порушення порядку розкриття інформації на фондовому ринку (ст. 163^{11} КУпАП).

	3. Незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових повноважень (ст. 172^8 КУпАП). 4. Порушення законодавства у сфері захисту персональних даних (ст. 188^{39} КУпАП). 5. Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію (ст. 212^5 КУпАП). **Література:** допоміжна:1 – 12. **Завдання на СРС:** вирішення задач (визначається викладачем згідно з додатком до робочої програми кредитного модуля).
8	**Тема 3.2. Адміністративно-правове забезпечення доступу до інформації** 1.Відмова від надання чи несвоєчасне надання екологічної інформації (ст. 91^4 КУпАП). 2.Порушення законодавства про захист прав споживачів (ст. 156^1 КУпАП). 3. Приховування інформації про діяльність емітента (ст. 163^5 КУпАП). 4. Порушення законодавства про державну таємницю (ст. 212^2 КУпАП). 5. Порушення права на інформацію та права на звернення (ст. 212^3 КУпАП) **Література:** допоміжна:1-12. **Завдання на СРС:** вирішення задач (визначається викладачем згідно з додатком до робочої програми кредитного модуля).
9	**Тема 3.3. Адміністративно-правове забезпечення захисту інформації у сфері використання інформаційних технологій** 1.Порушення Правил надання та отримання телекомунікаційних послуг (ст. 148^1 КУпАП). 2.Порушення порядку та умов надання послуг зв'язку в мережах загального користування (ст. 148^2 КУпАП). 3.Порушення правил про взаємоз'єднання телекомунікаційних мереж загального користування (ст. 148^5 КУпАП). 4.Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем (ст. 212^6 КУпАП). **Література:** допоміжна: 1-13. **Завдання на СРС:** вирішення задач (визначається викладачем згідно з додатком до робочої програми кредитного модуля).

6. Лабораторні заняття (комп'ютерний практикум)

Не передбачено навчальним планом.

7. Самостійна робота

Зміст кредитного модуля не передбачає тем для самостійного вивчення.

8. Індивідуальні завдання

Опрацьовуючи навчальний матеріал кредитного модуля «Публічно-правова охорона інформаційної безпеки», студенти виконують індивідуальне семестрове завдання шляхом підготовки реферату з певної теми. Виконання реферату сприяє поглибленню і розширенню теоретичних знань студентів з окремих тем дисципліни, розвиває навички самостійної роботи з навчальною та науковою літературою, сприяє формуванню вміння використовувати знання для вирішення відповідних практичних завдань. Реферат виконується студентами самостійно із забезпеченням необхідних консультацій з окремих питань з боку викладача. Після підготовки реферату студент має його захистити. Терміни видачі, виконання і захисту реферату визначаються графіком, що розробляється випусковою кафедрою на кожний семестр. Приблизна тематика рефератів наводиться у додатку № 2 до робочої програми кредитного модуля.

9. Контрольні роботи

Метою модульної контрольної роботи (МКР) є закріплення студентами навчального матеріалу модуля, а також контроль рівня знань студентів після вивчення певної логічно завершеної частини робочої програми кредитного модуля.

МКР складається з трьох частин, кожна тривалістю в 1 академічну годину. Перша частина МКР виконується студентами після завершення вивчення першого розділу робочої програми за матеріалом цього розділу. Друга частина МКР виконується студентами після завершення вивчення другого розділу робочої програми за відповідним навчальним матеріалом. Третя частина МКР виконується студентами після завершення вивчення третього розділу робочої програми за відповідним навчальним матеріалом.

Виконання кожної частини МКР полягає у вирішенні задачі. Варіанти і завдання на МКР наводяться у додатку до робочої програми кредитного модуля.

10. Рейтингова система оцінювання результатів навчання

Рейтингова система оцінювання результатів навчання (РСО) є додатком № 1 до робочої програми кредитного модуля.

11. Методичні рекомендації

При викладенні навчального матеріалу кредитного модуля, зважаючи на відносно невеликий за часом обсяг лекційних занять, доцільно зосереджувати увагу на висвітленні змісту ознак основного складу відповідного правопорушення (родовий об’єкт, ознаки об’єктивної і суб’єктивної сторони), розмежування схожих юридичних складів. Слід акцентувати увагу також на

важливих і актуальних для студентів питаннях з практики застосування відповідних правових норм.

Викладаючи лекційний матеріал, варто, по можливості, уникати вживання дат і номерів нормативних та інших документів, невиправданого «теоретизування», оскільки це, як правило, не завжди позитивно сприймається студентами, заважає ефективному засвоєнню основного навчального матеріалу. Окрім того, певні правові поняття і категорії можуть вимагати додаткового пояснення для студентів, про що необхідно пам'ятати.

На лекційних і семінарських заняттях доцільно використовувати графічний матеріал, який дозволяє наочно показати структуру складу злочину, механізм його вчинення, а також охарактеризувати структурні, функціональні, причинно-наслідкові, кореляційні та інші зв'язки у складних системах.

На семінарському занятті викладач, організовуючи дискусію, повинен намагатись залучити до обговорення питання чи проблеми більшу кількість студентів академічної групи (а не лише найактивнішу її частину). При цьому слід запобігати виникненню конфліктних ситуацій, спрямовуючи дискусію у конструктивному напрямі. На семінарські заняття серед іншого доцільно виносити ті правові питання, які мають практичне значення для студентів. На семінарських заняттях бажано застосовувати з навчальною метою моделювання конкретних життєвих ситуацій з певним юридичним змістом (наприклад, фабули вчинених правопорушень). Виступаючи в якості учасників таких ситуацій та розв'язуючи практичні завдання, оцінюючи конкретні ситуації, студенти зможуть краще засвоїти навчальний матеріал, виробити практичні навички застосування своїх правових знань.

Готуючись до семінарського заняття, студент має обов'язково опрацювати лекційний матеріал певної теми, ознайомитись зі змістом матеріалу підручника. При виникненні питань, виявленні незрозумілих положень необхідно обов'язково обговорити їх з викладачем. На семінарському занятті навіть добре підготовлений студент не повинен залишатись пасивним спостерігачем, а активно включатись у обговорення питання. Якщо ж студент не ознайомився з навчальним матеріалом, йому варто уважніше слухати виступаючих, і завдяки отриманій інформації намагатись компенсувати недоліки підготовки до заняття. Не слід відмовлятись від відповіді на питання викладача. Навіть якщо студент не знає відповіді, доцільно спробувати відповісти, висловити свою думку, виходячи з власних знань, досвіду, логіки запитання тощо. При цьому не треба боятися помилитися – одним з важливих завдань вивчення гуманітарних дисциплін є вироблення вміння логічно мислити і відповідно висловлювати власні думки. Однак, варто пам'ятати, що незнання матеріалу дисципліни є суттєвим недоліком роботи студента і буде негативно впливати на його загальний рейтинг. Відповідальне ставлення щодо підготовки на кожне семінарське заняття дає змогу не лише правильно засвоїти навчальний матеріал, але й заощадити зусилля при проходженні семестрового контролю.

Важливим у належній підготовці студента є вироблення у нього вміння працювати із законодавством, нормативно-правовими актами, іншими документами, які мають юридичне значення. Ознайомлюючись із новим для

себе законом, кодексом, постановою, інструкцією та ін. слід, насамперед, намагатись виявити сферу їх застосування (тобто, зміст суспільних відносин, які ними врегульовуються), мету і завдання їх створення, наскільки детально певний нормативний акт врегульовує відповідні відносини. Необхідно ознайомитись зі структурою документа, намагаючись зрозуміти логіку його побудови (тобто, викладення нормативного матеріалу) та зміст основних положень. Такий аналіз дозволить студенту не лише краще засвоїти інформацію, що міститься у документі, але й в подальшому швидше знаходити потрібну правову норму при виникненні, наприклад, певного практичного юридичного питання. На заняттях викладач має давати загальну характеристику основних нормативно-правових актів, які стосуються теми заняття, наочно розкривати їх структуру і зміст головних положень.

Якщо студента в процесі його самостійної роботи або аудиторних занять зацікавило певне конкретне питання або проблема, доцільно дослідити її детальніше шляхом, зокрема, виконання реферату з цієї проблематики. Написання реферату не повинно ґрунтуватись лише на матеріалі лекції або підручника, необхідно використовувати додаткову (в тому числі наукову) літературу, інформацію доступних нормативно-правових актів, публікації у періодичних виданнях тощо.

12. Рекомендована література

12.1. Базова

1. Конституція України // Відомості Верховної Ради України. – 1996. – №30. – Ст. 141.
2. Бєляков К.І. Інформація в праві : теорія і практика / К. І. Бєляков ; Державний НДІ Міністерства внутрішніх справ України. – К. : КВІЦ, 2006. – 118 с.
3. Бєляков К.І. Інформатизація в Україні : проблеми організаційного, правового та наукового забезпечення : монографія.– К. : КВІЦ, 2008. – 576с.
4. Горбулін, В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія / В. П. Горбулін [и др.] ; Рада національної безпеки і оборони України, Інститут проблем національної безпеки. – К. : Інтертехнологія, 2009. – 164 с.
5. Горбулін, В.П. Проблеми захисту інформаційного простору України : монографія / В. П. Горбулін, М. М. Биченок ; Інститут проблем національної безпеки, Рада національної безпеки і оборони України. - К. : Інтертехнологія, 2009. - 135 с.
6. Дзьобань О.П. Філософія інформаційних комунікацій : монографія / О. П. Дзьобань ; Нац. акад. прав. наук України, Н.-д. центр прав. інф-ки. - Х. : Майдан, 2012. - 223 с.
7. Згуровський М.З. Розвиток інформаційного суспільства в Україні : правове регулювання у сфері інформаційних відносин / М. З. Згуровський [и др.] ; Національний технічний ун-т України "Київський політехнічний ін-т". - К. : НТУУ "КПІ", 2006. - 544 с.

8. Згуровский М.З. Основы устойчивого развития общества [Текст] : курс лекций в 2 ч. / М.З. Згуровский, Г.О. Статюха. – К.: НТУУ «КПИ», 2010. – ч. 1. – 464 с.
9. Інформаційне суспільство: дефініції: людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція / В. М. Брижко [та ін.]. - К. : Інтеграл, 2002. - 220 с.
10. Кормич Б.А. Інформаційне право : підруч. для студ. вищ. навч. закл. / Б. А. Кормич. - Х. : Бурун і К, 2011. - 333 с.
11. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції : навч. посібник / В. А. Ліпкан [и др.] ; Київський національний ун-т внутрішніх справ. Кафедра міжнародних відносин та національної безпеки. - К. : КНТ, 2006. - 280 с.
12. Марущак А.І. Інформаційне право: доступ до інформації : навч. посіб. для студ. ВНЗ / А. І. Марущак. - К. : КНТ, 2007. - 531 с.
13. Марущак А.І. Інформаційне право України : Підручник. – К.: Дакор, 2011. – 456 с.
14. Нормативно-правове забезпечення інформаційної безпеки : навч. посіб. для студ. вищ. навч. закл., які навчаються за галуззю знань "Безпека інформаційних та коммунікаційних систем" / С. М. Головань [та ін.] ; [під. ред. В. О. Хорошко]. - Луганськ : Ноулідж, 2012. - 479 с.
15. Основи інформаційного права України : навч. Посіб. / В.С. Цимбалюк, В.Д.Гавлоський, В.М.Брижко та ін. ; за ред. М.Я.Швеця, Р.А.Калюжного, та П.В.Мельника. 2-ге вид., переробл. і допов. – К. : Знання, 2009. – 414 с.
16. Письменицький А.А. Загальна теорія інформаційного права: монографія / А. А. Письменицький, В. Д. Гапотій. – Мелітополь : Вид. будинок ММД, 2012. – 299 с.
17. Правовое обеспечение информационной безопасности: учеб. пособие для студ. вузов, обуч. по спец. 075200 - Компьютерная безопасность, 075500 – Комплексное обеспечение информационной безопасности автоматизированных систем, 075600 - Информационная безопасность телекоммуникационных систем / С. Я. Казанцев [и др.] ; ред. С. Я. Казанцев. - М. : Академия, 2005. - 238 с.
18. Селезньова О.М. Теоретико-методологічні основи інформауційного права Україні : монографія / О.М. Селезньова. – Чернівці : «Місто», 2014. – 408 с.
19. Соціально-правові основи інформаційної безпеки : навч. посіб. / В. М. Петрик [та ін.] ; ред. В. В. Остроухов ; Українська академія наук, Державний ун-т інформаційно-комунікаційних технологій. - К. : Росава, 2007. - 496 с.
20. Фурашев В.М. Системна інформатизація процесів підтримки прийняття рішень : монографія / В. М. Фурашев ; Наук.-дослід. центр прав. інф-ки Акад. прав. наук України. - К. : Синопсис, 2009. - 222, [2] с.
21. Харченко Л.С. Інформаційна безпека України : глосарій / Л. С. Харченко [и др.] ; заг. ред. Р. А. Калюжний. - К. : Текст, 2004. - 135 с.

22. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: підруч. для студ. напряму підготов. "Безпека інформаційних і комунікаційних систем" вищ. навч. закл. / [О. К. Юдін] ; Нац. авіац. ун-т. - К. : НАУ, 2011. - 639 с.
23. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики : монографія /Р.А. Калюжний, В.О.Шамрай, М.Я.Швець та ін. / За ред. Р.А. Калюжного і В.О.Шамрая. – Київ, 2002. – 296 с.

12.2. Допоміжна

До розділу 1

1. Антонов В.М. Інтелектуальна власність і комп'ютерне авторське право / В. М. Антонов. - 2-е вид., стер. - К. : КНТ, 2006. - 520 с.
2. Богуш В.М. Інформаційна безпека держави : [навч. посіб.] / В. М. Богуш, О. К. Юдін. - К. : МК-Прес, 2005. - 432 с.
3. Богуш В.М. Теоретичні основи захищених інформаційних технологій : навч. посіб. / В. М. Богуш, О. А. Довидьков, В. Г. Кривуца. - К. : [ДУІКТ], 2010. - 454 с.
4. Богуш В.М.Основи інформаційної культури : навч. посіб. / В. М. Богуш, О. Й. Куляниця. - К. : ДУІКТ, 2011. - 287 с.
5. Брижко В.М.. Е-боротьба в інформаційних війнах та інформаційне право / В. М. Брижко [и др.] ; Академія правових наук України. Науково-дослідний центр правової інформатики. - К. : НДЦПІ АПрН України, 2007. - 233 с.
6. Гнатюк С.О. Безпека інформації в інформаційно-комунікаційних системах: конспект лекцій : для студентів ВНЗ, які навчаються за напрямом 6.170103 "Управління інформаційною безпекою" / С. О. Гнатюк, М. О. Рябий ; Нац. авіац. ун-т, Каф. безпеки інформ. технологій, Європ. ун-т, Каф. орг. комплекс. захисту інформації. - Київ : НАУ, 2013. - 131 с.
7. Гороховський О.І. Інтелектуальна власність в галузі комп`ютерних технологій : навч. посіб. для студ. спец. "Компьютерні системи та мережі", "Інтелектуальні системи прийняття рішень", "Програмне забезпечення автоматизованих систем", "Захист інформації в компьютерних системах та мережах", "Адміністративний менеджмент у сфері захисту інформації з обмеженим доступом" / О. І. Гороховський, І. С. Колесник ; Вінницький національний технічний ун-т. - Вінниця : ВНТУ, 2007. - 146 с.
8. Гуз А.М. Історія захисту інформації в Україні та провідних країнах світу : навч. посібник / А. М. Гуз. - К. : КНТ, 2007. - 255 с.
9. Гурковський В.І. Державне управління розбудовою інформаційного суспільства в Україні (історія, теорія, практика) : монографія / Гурковський Володимир Ігорович. - К. : [Науковий світ], 2010. - 396 с.
10. Дзьобань О.П. Інформаційне насильство та безпека: світоглядно-правові аспекти : монографія / О. П. Дзьобань, В. Г. Пилипчук ; Нац. акад. прав. наук України, Н.-д. центр прав. інформатики, Ін-т дослідж. пробл. держ. безпеки. - Х. : Майдан, 2011. - 244 с.

11. Дроб'язко В.С. Охорона баз данних: міжнародні, регіональні, національні аспекти : монографія / В. С. Дроб'язко ; Акад. правових наук України, НДІ інтелект. власності. - К. : Лазуріт-Поліграф, 2008. - 132 с.
12. Замула О.А. Нормативно-правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації : учб. посіб. / О. А. Замула, Ю. І. Горбенко, О. І. Шумов ; Харк. нац. ун-т радіоелектрон. - Х. : ХНУРЕ, 2010. - 248 с.
13. Інтелектуальна власність у сфері захисту інформації : [підруч.] / С. М. Головань [и др.] ; ред. В. О. Хорошко ; Державний ун-тінформаційно-комунікаційних технологій. - К. : ДУІКТ, 2009. - 177 с.
14. Інформаційні війни. Моніторинг теленовин та медіатехнологій під час президентської кампанії-2004 в Україні / заг. ред. Н. Лигачова. - К. : Телекритика, 2005. - 192 с.
15. Інформаційно-психологічне протиборство (еволюція та сучасність) : монографія / Я. М. Жарков [та ін.] ; Військ. ін-т Київ. нац. ун-ту ім. Тараса Шевченка. - К. : Віпол, 2013. - 247 с.
16. Кіслов Д.В. Інформаційні війни : монографія / Д. В. Кіслов ; Київ. нац. торг.-екон. ун-т. - К. : [б. в.], 2013. - 300 с.
17. Кіслов Д.В. Сучасні медіа та інформаційні війни : [монографія] / Д. В. Кіслов ; Київ. міжнар. ун-т, Ін-т журналістики. - 2-е вид. - К. : Леся, 2013. - 239 с.
18. Комп'ютерний тероризм: практика запобігання, протидії, розслідування : кримінолого-криміналістичний аналіз та правові, управлінські і тактико-технологічні засади запобігання, протидії, розслідування комп'ютерних терористичних актів: навч. посібник / П. Д. Біленчук [и др.] ; заг. ред. П. Д. Біленчук ; Хмельницький держ. центр науково-технічної і економічної інформації, Київський національний ун-т внутрішніх справ. - Хмельницький : Хм. ЦНТЕІ, 2008. - 258 с.
19. Кормич Б.А. Інформаційна безпека: організаційно-правові основи : навч. посібник для студ. вищих навч. закл. / Б. А. Кормич. - К. : Кондор, 2004. - 384 с
20. Манойло А.В. Государственная информационная политика в условиях информационно-психологической войны / А. В. Манойло [и др.]. - 2-е изд., стер. - М. : Горячая линия-Телеком, 2007. - 542 с.
21. Мережі і мережні війни: Майбутнє терору, злочинності та бойових дій / пер. з англ. А. Іщенко ; ред. Д. Арквілли, Д. Ронфельдт. - К. : Видавничий дім "Києво-Могилянська академія", 2005. - 352 с.
22. Національний інформаційний суверенітет у контексті розвитку новітніх інформаційних технологій : [монографія] / [Онищенко О. С. та ін.] ; Нац. акад. наук України, Нац. б-ка України ім. В. І. Вернадського. - К. : НБУВ, 2011. - 160 с.
23. Нестеренко О.В. Безпека інформаційного простору державної влади. Технологічні основи: монографія / О. В. Нестеренко ; НАН України, Ін-т пробл. реєстрації інформації. - К. : Наукова думка, 2009. - 352 с.

24. Павлов І.М. Проектування комплексних систем захисту інформації : підруч. для студ. вищ. навч. закл., які навчаються за галуззю знань "Інформаційна безпека" / І. М. Павлов, В. О. Хорошко ; Держ. служба спец. зв'язку та захисту інформації, Військ. ін-т телекомунікацій таінформатизації Нац. техн. ун-ту України "Київ. політехн. ін-т", Держ. ун-т інформ.-комунікац. технологій. - К. : ВІТІ : ДУІКТ, 2011. - 244 с.
25. Попов К.Л. Інформаційно-психологічні війни : перспективи криміналізації // Наука кримінального права в системі міждісциплінарних зв'язків : матеріали міжнар. наук.-практ конф., 9-10 жовт. 2014 р. / редкол.: В.Я.Тацій (голов. ред.), В.І.Борисов (заст. голов. ред.) та ін. – Х.: Право, 2014. – 536 с.
26. Почепцов Г.Г. Контроль над разумом. – К.: Видавничий дім «Києво-Могилянська авадемія», 2012. – 351 с.
27. Правове забезпечення інформаційної діяльності в Україні / Ю. С. Шемшученко [та ін.] ; заг. ред. Ю. С. Шемшученко, І. С. Чиж ; Ін-т держави і права ім. В.М.Корецького НАН України, Держ. ком. телебачення і радіомовлення України. - К. : ТОВ "Вид-во "Юридична думка", 2006. - 384 с.
28. Правові основи охорони інформації / В. Ф. Авраменко [та ін.] ; ред. В. О. Хорошко. - К. : ТОВ "ПоліграфКонсалтинг", 2003. - 176 с.
29. Правові основи охорони інформації : підруч. для студ. вищ. навч. закл., які навчаються за напрямом "Інформаційна безпека" / З. Б. Живко [и др.] ; заг. ред. В. О. Хорошко ; Державний ун-т інформаційно-комунікаційних технологій. - Вид. 2-ге, допов. і переробл. - К. : ДУІКТ, 2009. - 355 с.
30. Розвиток ресурсної бази вітчизняного інформаційного середовища : [монографія] / [О. С. Онищенко та ін. ; бібліогр. ред. І. П. Антоненко] ; Нац. акад. наук України, Нац. б-ка України ім. В. І. Вернадського. - К. : [б. в.], 2012. - 245 с.
31. Системна інформатизація законотворчої та правоохоронної діяльності / Верховна Рада України. Апарат. Управління комп'ютеризованих систем, Академія правових наук України. Науково-дослідний центр правової інформатики ; ред. В. В. Дурдинець [та ін.]. - К. : Навчальна книга, 2005. - 640 с.
32. Слепцов В.І. Правове та нормативне забезпечення інформаційної безпеки : [монографія] / В. І. Слепцов ; Запоріз. нац. техн. ун-т. - Запоріжжя : ЗНТУ, 2010. - 155 с.
33. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій : навч. посібник / В. М. Петрик [та ін.]. - К. : Росава, 2006. - 208 с.
34. Технології комплексного захисту інформації : навч. посібник / уклад. Л. Ф. Політанський [та ін.] ; Чернівецький національний ун-т ім. Юрія Федьковича. - Чернівці : Рута, 2007. - 140 с.

До розділу 2

1. Азаров Д.С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) : монографія / Д. С. Азаров ; Національний ун-т "Києво-Могилянська академія", Державний НДІ МВС України. - К. : Атіка, 2007. - 304 с.
2. Безпека комп'ютерних систем. Злочинність у сфері комп'ютерної інформації та її попередження / М. С. Вертузаєв [и др.] ; ред. О. П. Снігерьов ; Запорізький юридичний ін-т МВС України, Національна академія внутрішніх справ України. - Запоріжжя : Павел, 1998. - 315 с
3. Букалерова Л.А. Уголовно-правовая охрана официального информационного оборота : монография / Л. А. Букалерова ; ред. В. С. Комиссаров, Н. И. Пикуров. - М. : Юрлитинформ, 2006. - 356 с.
4. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія / В. М. Бутузов ; Рада нац. безпеки і оборони України, Міжвід. наук.-дослід. центр з пробл. боротьби з організ. злочинністю. - К. : КИТ, 2010. - 408 с.
5. Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій : монографія / І. Ф. Хараберюш [и др.] ; Донецький юридичний ін-т Луганського держ. ун-ту внутрішніх справ, Національний ун-т держ. податкової служби України. - К. : КНТ, 2007. - 195 с.
6. Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій : монографія / І. Ф. Хараберюш [и др.] ; Донецький юридичний ін-т Луганського держ. ун-ту внутрішніх справ, Національний ун-т держ. податкової служби України. - К. : КНТ, 2007. - 195 с.
7. Голубєв В.О. Інформаційна безпека: проблеми боротьби з кіберзлочинами / В. О. Голубєв ; Гуманітарний ун-т "Запорізький ін-т державного та муніципального управління". - Запоріжжя : [б.в.], 2003. - 250 с.
8. Голубєв В.О. Інформаційна безпека: проблеми боротьби з кіберзлочинами / В. О. Голубєв ; Гуманітарний ун-т "Запорізький ін-т державного та муніципального управління". - Запоріжжя : [б.в.], 2003. - 250 с.
9. Карчевський М.В. Кримінально-правова охорона інформаційної безпеки України : монографія / М. В. Карчевський ; Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. - Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка , 2012. - 526 с.
10. Карчевський М.В. Злочини у сфері використання комп'ютерної техніки : навч. посіб. / М. В. Карчевський ; Луганський держ. ун-т внутрішніх справ. - Луганськ : РВВ ЛДУВС, 2006. - 192 с.
11. Карчевский Н.В., Музыка А.А. Неправомерный доступ к компьютерной информации: уголовно-правовое исследование : монография. – К. : «МП Леся», 2015. – 208 с.
12. Коваленко В.В. Розслідування шахрайств і пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків : монографія / В. В.Коваленко, А. І. Анапольська ; Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. - Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2013. - 222, [1] с.

13. Комп'ютерний тероризм: практика запобігання, протидії, розслідування : кримінолого-криміналістичний аналіз та правові, управлінські і тактико-технологічні засади запобігання, протидії, розслідування комп'ютерних терористичних актів: навч. посібник / П. Д. Біленчук [и др.] ; заг. ред. П. Д. Біленчук ; Хмельницький держ. центр науково-технічної і економічної інформації, Київський національний ун-т внутрішніх справ. - Хмельницький : Хм. ЦНТЕІ, 2008. - 258 с.
14. Комп'ютерний тероризм: суперхакери, кібер-терористи, кібер-криміналісти : монографія / П. Д. Біленчук [та ін.] ; заг. ред. П. Д. Біленчук. - К. : Наука і життя, 2008 . - (Управління. Інновації. Безпека).
15. Кримінальне право України. Загальна частина: Підручник / Баулін Ю. В., Борисов В. І., Кривоченко Л. М. та ін.; за ред. проф. В. В. Сташиса, В. Я. Тація. – Х.: Право, 2010. – 456 с.
16. Кримінальний кодекс України (Прийнятий 5 квітня 2001 р. на сьомій сесії Верховної Ради): Офіційний текст. – К.: Видавець Паливода А.В., 2015. – 212 с.
17. Кримінальний кодекс України: Науково-практ. коментар / Баулін Ю. В., Борисов В. І., Гавриш С. Б. / В. В. Сташис, В. Я. Тацій (заг.ред.). — Х.: Одіссей, 2007. — 1183с.
18. Кримінальний кодекс України: Науково-практичний коментар. / Відп. ред. Є.Л. Стрельцов. – Х.: ТОВ "Одісей", 2008.
19. Музика А.А. Законодавство України про кримінальну відповідальність за "комп'ютерні" злочини: науково-практичний коментар і шляхи вдосконалення / А. А. Музика, Д. С. Азаров. - К. : Паливода А. В. [вид.], 2005. - 119 с.
20. Науково-практичний коментар до Кримінального кодексу України. / За заг. ред. П. П. Андрушка, В. Г. Гончаренка, Є. В. Фесенка. – К.: Дакор, 2008.
21. Науково-практичний коментар до Кримінального кодексу України: у 2 т. / П.П. Андрушко (ред.). Т. 1: – К.: Правова єдність, 2009. — 964 с.; Т. 2: – К.: Правова єдність, 2009. — 624с.
22. Науково-практичний коментар Кримінального кодексу України / За ред. М. І. Мельника, М. І. Хавронюка. – К.: Атіка, 2007.
23. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / Бутузов В. М. [та ін. ; за ред.: Б. В. Романюка, Є. Д. Скулиша] ; Рада нац. безпеки і оборони України, Міжвід. наук.-дослід. центр з пробл. організованої злочинності, Служба безпеки України, Нац. акад. служби безпеки України. - К. : [б. в.], 2011. - 404 с. : рис., табл. - Бібліогр.: с. 264-310.
24. Петрик Є.О. Практичні аспекти розкриття інформації на фондовому ринку України / Петрик Є. О., Ступак О. В. - Київ : Емкон, 2014. - 131 с.
25. Пикуров Н.И. Подлог и другие преступные посягательства на официальный документооборот : учеб. пособ. / Н. И. Пикуров, Л. А. Букалерова ; МВД РФ. Волгоградская академия. - Волгоград : [б.и.], 2001. - 113 с.
26. Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та

шляхи вирішення : матеріали всеукр. наук.-практ. конф., 12 листоп. 2010 р. / Донец. юрид. ін-т Луган. держ. ун-ту внутр. справ ім. Е. О. Дідоренка, Каф. ОРД ф-ту кримін. міліції. - Донецьк : [ДЮІ ЛДУВС], 2010. - 207 с.

27. Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення : матеріали всеукр. наук.-практ. конф., 9 груд. 2011 р. / Донец. юрид. ін-т МВС України, Каф. операт.-розшук. діяльн. ф-ту кримін. міліції. - Донецьк : ДЮІ МВС України, 2012. - 263 с.
28. Радутний О.Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну або банківську таємницю : монографія / О. Е. Радутний ; Національна юридична академія України ім. Ярослава Мудрого. - Х.: Ксілон,2008. - 202с.
29. Савінова Н.А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти: монографія /Савінова Н.А. - К. : ДКС, 2012. - 342 с.
30. Салтевский М.В. Проблемы противодействия преступности в сфере компьютерных технологий : науч.-практ. пособие / М. В. Салтевский, А. Н. Литвинов, Н. Г. Чернец. - М. : [Юркнига], 2006. - 96 с.
31. Системи охорони державної таємниці : підручник / С. М. Головань [та ін.] ; Східноукр. нац. ун-т ім. Володимира Даля. - Луганськ : Вид-во СНУ ім. В. Даля, 2012. - 294 с.
32. Системна інформатизація правоохоронної діяльності : у 2 кн. / Науково-дослідний центр правової інформатики Академії правових наук України, Департамент інформаційних технологій МВС України. - К. : НДЦПІ АПрН України, 2006 . - Кн. 1 / М. Швець [та ін.] ; ред. В. Дурдинець [та ін.]. - [Б. м.] : [б.в.], 2006. - 288 с. Кн. 2 : Європейські нормативно-правові акти та підходи до упорядкування суспільних інформаційних відносин у зв'язку з автоматизованою обробкою даних у правоохоронній діяльності / упоряд. М. Швець [та ін.] ; ред. М. Швець, Б. Романюк. - [Б. м.] : [б.в.], 2006. - 510 с.
33. Тарасюк А.В. Доказування у справах про несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку у стадії досудового розслідування : монографія / А. В. Тарасюк ; Нац. акад. Служби безпеки України. - Х. : ФІНН, 2011. - 191 с.
34. Трембіцький А.М. Правові основи захисту комерційної таємниці : курс лекцій / А. М. Трембіцький ; [Хмельниц. ін-т Міжрегіон. акад. упр. персоналом]. - Хмельницький : [б. в.], 2010. - 179 с.
35. Щербаковський М.Г. Розслідування комп'ютерних злочинів : навч. посіб. / М. Г. Щербаковський, Д. В. Пашнєв. - Х. : Харк. нац. ун-т внутр. справ, 2010. - 112 с. - Бібліогр.: с. 89-94.

До розділу 3

1. Ботвінкін О.В. Інформація з обмеженим доступом, що не є державною таємницею, в законодавстві України: аналітичний огляд / О. В. Ботвінкін, В. П. Ворожко. - К. : Видавництво Національної академії СБУ, 2006. - 96 с.
2. Дергачов В.С. Науково-практичні засади захисту інформації з обмеженим доступом у трудових правовідносинах : монографія / В. С. Дергачов ; Харк. нац. автомобіл.-дорож. ун-т. - Х. : ХНАДУ, 2011. - 160 с.
3. Ліпкан В.А. Адміністративно-правовий режим інформації з обмеженим доступом в Україні : монографія / В. А. Ліпкан, В. Ю. Баскаков ; за заг. ред. В. А. Ліпкана ; Глобал. орг. союзниц. лідерства, Акад. безпеки відкр. суспва, Акад. наук вищ. освіти України. - К. : О. С. Ліпкан [вид.], 2013. - 342 с.
4. Марущак А.І. Правові основи захисту інформації з обмеженим доступом : курс лекцій / А. І. Марущак. - К. : КНТ, 2007. - 208 с.
5. Марущак А.І. Правомірні засоби доступу громадян до інформації : науково-практ. посібник / А. І. Марущак ; Київське обласне творче об'єднання "Культура". - Біла Церква : Буква, 2006. - 431 с.
6. Нестеренко О. Право на доступ до інформації: теорія та практика / О. Нестеренко, О. Северин ; Харківська правозахисна група. - Х. : Права людини, 2008. - 347 с.
7. Нестеренко О.В. Інформація в Україні: право на доступ / Оксана Нестеренко. - Х. : Акта, 2012. - 306 с. - Бібліогр.: с. 250-276.
8. Олійник О.В. Теоретико-методологічні засади адміністративно-правового забезпечення інформаційної безпеки України : монографія / О. В. Олійник ; Ін-т законодавства Верховної Ради України. - К. : Укр. пріоритет, 2012. – 399 с.
9. Організаційно-правові основи захисту інформації з обмеженим доступом : навч. посібник для студ. вищих навч. закл. / А. Б. Стоцький [та ін.] ; заг. ред. В. С. Сідак ; Національна академія СБ України, Інститут захисту інформації з обмеженим доступом, Європейський ун-т. - К. : Вид-во Європейського ун-ту, 2006. - 232 с.
10. Організаційно-правові основи охорони конфіденційної інформації, що є власністю держави : навч. посібник / В. В. Макаренко [и др.] ; Національна академія Служби безпеки України. - К. : Науково-видавничий відділ Національної академії СБ України, 2008. - 73 с.
11. Стоєцький О.В. Адміністративна відповідальність за правопорушення у сфері інформаційної безпеки України: автореф. дис. ... канд. юрид. наук : 12.00.07 / Держ. вищ. навч. закл. "Запоріз. нац. ун-т". - Запоріжжя, 2013. – 20 с.
12. Чуприна О.В. Адміністративна відповідальність за порушення права на інформацію : автореф. дис. ... канд. юрид. наук : 12.00.07 / Чуприна Олена Василівна ; Нац. авіац. ун-т. - К., 2013. - 20 с.
13. Шепета О.В. Адміністративно-правові засади технічного захисту інформації : монографія / О. В. Шепета ; Акад. наук вищ. освіти України, Global organization of allied leadership, Acad. of open society security. - К. : О. С. Ліпкан, 2012. - 295 с.

13. Інформаційні ресурси

1. Офіційний веб-портал судової влади України http://court.gov.ua/
2. Офіційний веб-портал Верховної Ради України http://rada.gov.ua/
3. Офіційний веб-сайт МВС України http://mvs.gov.ua/
4. Єдиний державний реєстр судових рішень http://www.reyestr.court.gov.ua
5. Реєстр друкованих ЗМІ та інформаційних агентств як суб'єктів інформаційної діяльності http://dzmi.informjust.ua
6. Реєстр. Винаходи та корисні моделі. Знаки для товарів і послуг. Промислові зразки. Інші бази даних Інституту промислової власності http://www.uipv.org/ua/bases2.html
7. Державний реєстр телерадіоорганізацій http://www.nrada.gov.ua/ua/13720.html
8. Реєстр адміністративних послуг http://poslugy.gov.ua/AdminService/List
9. Реєстр організаторів державної експертизи у сфері технічного захисту інформаціїhttp://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=39524&cat_id=38689&ctime=1127826004742
10. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id=111290&cat_id=39181&mustWords=%D0%BF%D0%B5%D1%80%D0%B5%D0%BB%D1%96%D0%BA&searchPublishing=1
11. Перелік сертифікованих засобів криптографічного захисту інформаціїhttp://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id=39217&cat_id=39136
12. Перелік відомостей, що становлять службову інформацію і яким присвоюється гриф “Для службового користування” http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id=92345&cat_id=92339&mustWords=%D0%BF%D0%B5%D1%80%D0%B5%D0%BB%D1%96%D0%BA+%D1%81%D1%83%D0%B1&searchPublishing=1
13. Реєстр наукових організацій http://store.uintei.kiev.ua/reestr_new.html
14. Перелік об'єктів права інтелектуальної власності, включених до митного реєстру http://sfs.gov.ua/dovidniki--reestri--perelik/pereliki-/100237.html
15. Реєстр корпоративних прав держави http://www.spfu.gov.ua/_layouts/SPFUSiteDefinition/RegisterStateCorporateRights.aspx
16. База даних “Законодавство України”http://zakon4.rada.gov.ua/laws

Додаток 1
до робочої програми кредитного модуля
"Публічно-правова охорона інформаційної безпеки"

Рейтингова система оцінювання результатів навчання

Рейтинг студента з кредитного модуля «Публічно-правова охорона інформаційної безпеки» складається з балів, що отримуються за:

1) відповіді, вирішення задач та доповнення відповідей інших студентів у процесі дискусії на практичних заняттях;

2) модульну контрольну роботу (МКР), що складається з трьох частин.

Система рейтингових (вагових) балів та критерії оцінювання:

1. Робота на практичних заняттях (максимальна кількість балів на практичних заняттях складає 70:

Присутність не менш ніж на 80% проведених занять; активна участь на не менш ніж 80% відвіданих занять; надання переважно повних і аргументованих, логічно викладених відповідей, висловлення власної позиції з дискусійних питань або повністю правильним вирішенням задач з відповідним обгрунтуванням, у поєднанні зі слушними доповненнями відповідей інших студентів у процесі дискусії	60-70
Присутність не менш ніж на 70% проведених занять; активна участь на не менш ніж 70% відвіданих занять; надання переважно аргументованих відповідей або правильним вирішенням задач з незначними неточностями, порушеннями логіки викладення відповіді чи обґрунтування при вирішенні задачі	40-59
Присутність не менш ніж на 60% проведених занять; активна участь на не менш ніж 70% відвіданих занять; надання в цілому правильних, але неповних відповідей з декількома неточностями або помилками при вирішенні задачі	30-39
Присутність не менш ніж на 30% проведених занять; активна участь не менш ніж на 50% відвіданих занять; надання відповідей з чисельними значними похибками або вирішення задач з грубими помилками; неподання обгрунтування при вирішенні задачі	20-29
Присутність не менш ніж на 20% проведених занять; активна участь на відвіданих заняттях; надання відповідей, які свідчать про непідготовленість та незнання відповідного матеріалу	11-19
Присутність менш ніж на 20% проведених занять;	1-10
Відсутність на заняттях	0

2. Модульний контроль (ваговий бал однієї частини МКР – 10; максимальна кількість балів за МКР складає 30):

Повна, чітка, викладена в певній логічній послідовності відповідь на всі поставлені питання, що свідчить про глибоке розуміння суті питання, ознайомлення студента не лише з матеріалом лекцій, але й з підручником та додатковою літературою; висловлення студентом власної позиції щодо дискусійних проблем, якщо такі порушуються у питанні	9-10
Не зовсім повна або не достатньо чітка відповідь на всі поставлені питання, що свідчить про правильне розуміння суті питання, ознайомлення студента з матеріалом лекцій та підручника; незначні неточності у відповідях	6-8
Відсутність відповіді на певні питання, або неправильна відповідь на них, що свідчить про поверхове ознайомлення студента з навчальним матеріалом або значні похибки у відповідях	3-5
Неправильна відповідь, що свідчить про незнання матеріалу, але намагання студента висловити власне розуміння суті поставленого питання	1-2
Відсутність відповіді	0

Розрахунок шкали (R) рейтингу:

Сума вагових балів контрольних заходів протягом семестру складає:

$$RD = 70 + 30 = 100 \text{ балів.}$$

*Необхідною умовою допуску до заліку є рейтинг (**RD**) не менше 40% від **R**, тобто 40 балів.* Студенти, які набрали протягом семестру 60 і більше балів (***RD ≥ 0,6 R)*** отримують залік так званим "автоматом" відповідно до набраного рейтингу.

Студенти, які набрали протягом семестру від 40 до 59 балів (***0,4 R ≤ RD < 0,6 R)*** виконують залікову контрольну роботу, яка складається з чотирьох завдань (трьох теоретичних питань і тестового завдання).

Критерії оцінювання залікової контрольної роботи.

Залікова контрольна робота (ваговий бал кожного завдання – 10, максимальна кількість балів - 40):

Повна, чітка, викладена в певній логічній послідовності відповідь на поставлене питання, що свідчить про глибоке розуміння суті питання, ознайомлення студента не лише з матеріалом лекцій, але й з підручником та додатковою літературою; висловлення студентом власної позиції щодо дискусійних проблем, якщо такі порушуються у питанні; правильне вирішення більше 80% тестового завдання	9-10
Не зовсім повна або не достатньо чітка відповідь на поставлене питання, що свідчить про правильне розуміння суті питання, ознайомлення студента з матеріалом лекцій та підручника, правильне вирішення від 60% до 80% тестового завдання	6-8

Поверхова відповідь, суттєві помилки у відповіді, правильне вирішення від 30% до 60% тестового завдання	3-5
Неправильна відповідь, що свідчить про незнання матеріалу, але намагання студента висловити власне розуміння суті поставленого питання, правильне вирішення до 30% тестового завдання	1-2
Відсутність відповіді, вирішення тестового завдання повністю неправильне	0

Для отримання студентом відповідних оцінок (ECTS та традиційних) його рейтингова оцінка (***RD***) переводиться згідно з таблицею:

RD	**Оцінка ECTS**	**Оцінка традиційна**
95 – 100	A – відмінно	Відмінно
85 – 94	B – дуже добре	Добре
75 – 84	C – добре	
65 – 74	D – задовільно	Задовільно
60 – 64	E – достатньо (задовольняє мінімальні критерії)	
RD < 60	FX – незадовільно	Незадовільно
RD < *40*	*F – незадовільно (потрібна додаткова робота)*	*Не допущений*

Додаток 2
до робочої програми кредитного модуля
"Публічно-правова охорона інформаційної безпеки"

ТЕМАТИКА РЕФЕРАТІВ

1. Інформація як предмет правопорушення
2. Зміст і співвідношення понять «інформаційна сфера», «інформаційне середовище», «інформаційна система», «інформаційне поле», «інформатизація»
3. Конституційно-правові підстави захисту інформації
4. Загальна характеристика публічно-правової охорони інформаційної безпеки у зарубіжних країнах
5. Глобалізація, інтернаціоналізація та інформаційна безпека
6. Основні положення законодавства ЄС щодо інформаційної безпеки
7. Правові механізми запобігання інформаційним війнам та інформаційному тероризму
8. Кримінальна відповідальність за публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади
9. Кримінальна відповідальність за ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію
10. Кримінальна відповідальність за злочини проти порядку охорони конфіденційної інформації про особу
11. Кримінальна відповідальність за незаконні дії з відомостями, які становлять комерційну, банківську таємницю чи інсайдерську інформацію
12. Кримінальна відповідальність надання неправдивих відомостей до органу ведення Державного реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців
13. Кримінальна відповідальність за незаконне знищення виборчої документації або документів референдуму
14. Кримінальна відповідальність за декларування недостовірної інформації
15. Кримінальна відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку
16. Кримінальна відповідальність за створення шкідливих програмних чи технічних засобів
17. Кримінальна відповідальність за несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в ЕОМ, автоматизованих системах, комп’ютерних мережах
18. Кримінальна відповідальність за несанкціоновані дії з інформацією, яка оброблюється в ЕОМ, АС, КМ
19. Кримінальна відповідальність за порушення правил експлуатації ЕОМ, АС, КМ

20. Кримінальна відповідальність за перешкоджання роботі ЕОМ, АС, КМ, МЕ шляхом масового розповсюдження повідомлень електрозв’язку
21. Кримінальна відповідальність за незаконне втручання в роботу автоматизованої системи документообігу суду (ст. 3761 КК України)
22. Незаконне використання інсайдерської інформації (ст. 1639 КУпАП)
23. Порушення порядку розкриття інформації на фондовому ринку (ст. 16311 КУпАП)
24. Незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових повноважень (ст. 1728 КУпАП)
25. Порушення законодавства у сфері захисту персональних даних (ст. 18839 КУпАП)
26. Порушення порядку обліку, зберігання і використання документів та інших носіїв інформації, які містять конфіденційну інформацію, що є власністю держави (ст. 2125 КУпАП)
27. Порушення законодавства про захист прав споживачів (ст. 1561 КпАП)
28. Порушення права на інформацію (ст. 2123 КпАП)
29. Порушення Правил надання та отримання телекомунікаційних послуг (ст. 1481 КУпАП)
30. Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем (ст. 2126 КУпАП)