СИЛАБУС
Кафедра кібербезпеки та математичного моделювання

Назва курсу	Нормативно-правове забезпечення інформаційної безпеки
Мова викладання	українська
Викладач	Петренко Тарас Анатолійович, доцент
Профайл викладача	Сайт кафедри: https://mmi.stu.cn.ua/personal-kafedry/ Google академія: https://scholar.google.com/citations?user=2bJE-4IAAAAJ&hl=ru
Контакти викладача	тел.: 0636419136, e-mail: mail_taras@ukr.net

1. Анотація курсу. Сьогодні будь-які суспільні взаємовідносини, професійна та повсякденна діяльність людини регулюється тими чи іншими нормативно-правовими документами, не стоїть осторонь і галузь кібербезпеки. Саме тому наявність знань основних положень нормативно-правових документів є обов'язковою для майбутньої успішної професійної діяльності в сфері захисту інформації.

На заняттях курсу «Проектування технічних засобів захисту інформації» студенти досліджують вітчизняне та зарубіжне законодавство в сфері кібербезпеки та захисту інформації. Аналізують українські та міжнародні стандарти в цій галузі. Намагаються критично осмислити існуючі нормативні документи та запропонувати свої корективи які зможуть вдосконалити існуюче нормативно-правове поле в сфері кібербезпеки та захисту інформації.

Успішне засвоєння дисципліни дозволяє магістру зі спеціальності 125 – Кібербезпека розширити коло застосування набутих раніше знань та практичних навичок для вирішення професійних задач організації захисту інформації, що неможливо без ґрунтовних знань в галузі нормативноо-правового забезпечення цієї діяльності.

2. Мета та цілі курсу - отримання студентами необхідних знань з нормативно-правових основ захисту інформації в Україні та світі та розвиток загальних та фахових компетентностей бакалаврів галузі знань 12 – Інформаційні технології, спеціальності 125 – Кібербезпека.

Навчальна дисципліна "Нормативно-правове забезпечення інформаційної безпеки" входить до циклу фахових дисциплін. Предметом вивчення є вітчизняне та зарубіжне законодавство що регулює взаємовідносини в сфері інформаційної безпеки. Дисципліна формує компетенції з правових основ захисту інформації в інформаційно–телекомунікаційних системах та покликана сформувати у студентів уявлення про правові передумови захисту інформації, цілісні знання про правові норми, що регламентують суспільні відносини з приводу захисту інформації в Україні та світі.

Зокрема, це такі загальні компетентності, як:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях;

КЗ 2. Знання та розуміння предметної області та розуміння професії;

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

Також, це такі фахові компетенції:

КФ 1. Здатність розробляти та впроваджувати законодавчу, нормативно-правову ба-

зу, державні і міжнародні вимоги, а також інтегрувати, аналізувати і використовувати сучасні світові практики та стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

КФ 7. Здатність розробляти, впроваджувати, супроводжувати системи аудиту та моніторингу якості бізнес/операційних процесів функціонування організації та системи управління інформаційною безпекою та/або кібербезпекою за вітчизняними і світовими нормами та стандартами.

КФ 8. Здатність проводити науково-освітню діяльність, розробляти та впроваджувати систему управління персоналом, а також проводити та планувати навчання працівників компанії і наукові дослідження в галузі інформаційних технологій у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації у відповідність вітчизняним та світовим стандартам галузі інформаційної та/або кібербезпеки.

3. Результати навчання:

Навчальна дисципліна «Нормативно-правове забезпечення інформаційної безпеки» має допомогти сформувати наступні програмні результати навчання:

ПРН 2. планувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

ПРН 3. використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

ПРН 4. аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

ПРН 5. реалізовувати процеси постійної самоосвіти і професійної сертифікації, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

ПРН 6. діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі у напрямах найкращих практик, технічних вимог та рекомендацій з управління інформаційною безпекою та /або кібербезпекою;

ПРН14. розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації. У результаті вивчення дисципліни студенти мають знати:

– поняття, види, правові ознаки, класифікацію інформації;

– законодавчі основи захисту інформації в Україні;

– правові особливості захисту різних видів інформації (державної таємниці, комерційної таємниці, банківської таємниці, персональної інформації тощо).

– нормативно-правові акти, які закріплюють визначальні положення щодо забезпечення інформаційної безпеки України

– основні положення нормативно-правових актів з інформаційної безпеки телекомунікаційних систем;

– основні положення законів України про електронний документообіг та електронний цифровий підпис

– підзаконні нормативні акти щодо електронного документообігу та електронного цифрового підпису

– НПА, які визначають порядок технічного захисту інформації в Україні.

Уміти:

– діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, в тому числі міжнародних в галузі інформаційної та/або кібербезпеки;

– аналізувати та розкривати особливості правового статусу видів інформації з обмеженим доступом;

– застосовувати на практиці здобуті знання, розуміти і застосовувати у повсякденній діяльності організаційно-правові основи захисту інформації;

– використовувати основні правові джерела щодо планування та реалізації заходів захисту інформації в ІТС відомств, установ, організацій Україні;

– виявляти недоліки у вітчизняній нормативно-правовій базі;

– здійснювати роботу з удосконалення нормативно-правового забезпечення галузі та її адаптацію до міжнародних вимог і стандартів.

4. Обсяг курсу. 3 кредити ECTS, що становить 90 годин роботи студентів, з них 60 годин самостійної роботи та 30 годин аудиторної роботи з викладачем.

Вид заняття	Загальна кількість годин
Лекції	16
Лабораторні заняття	14
Самостійна робота (РГР, наукові дослідження)	60

Тематика курсу

Змістовий модуль 1. Загальні положення нормативно-правового забезпечення інформаційної безпеки

1. Основи правового забезпечення інформаційної безпеки
2. Міжнародне законодавство в галузі інформаційної безпеки
3. Нормативно-правові акти що закріплюють основні положення інформаційної безпеки України
4. Нормативно-правове забезпечення охорони державної таємниці в Україні
5. Нормативно-правові акти щодо захисту конфіденційної інформації

Змістовий модуль 2. Спеціальне законодавство у галузі інформаційної безпеки

6. Нормативно-правові акти в сфері захисту інформації в телекомунікаційних системах
7. Нормативні документи з технічного захисту інформації
8. Законодавство в сфері електронного документообігу
9. Нормативно-правове забезпечення електронного цифрового підпису
10. Злочини в сфері інформаційної безпеки. Законодавче регулювання

5. Пререквізити. Дисципліна «Нормативно-правове забезпечення інформаційної безпеки» вивчається з опорою на знання студентів з інших нормативних-правових дисциплін таких як інформаційна безпека держави, основи національної безпеки, система охорони державної таємниці, організаційне забезпечення захисту інформації, організація спеціального діловодства та ін. Дисципліна «Нормативно-правове забезпечення інформаційної безпеки» є базовою для подальшої успішної професійної діяльності за спеціальністю, а також може використовуватися під час підготовки випускної кваліфікаційної роботи магістра.

6. Система оцінювання та вимоги

Загальна система оцінювання курсу	ECTS
Вимоги до курсового проекту	При перевірці та оцінюванні контрольної роботи враховується правильність виконання теоретичних та практичних завдань, самостійність виконання, вчасність здачі роботи та відповідність оформлення результатів діючим вимогам
Лабораторні заняття	Кожна виконана лабораторна робота оцінюється від 0 до 3-х балів. Кількість балів залежить від рівня теоретичних знань та практичних навичок студента за темою, самостійності виконання роботи та вчасності її захисту
Умови допуску до підсумкового контролю	Умовою допуску до екзамену є виконання та отримання хоча б мінімальної кількості балів з усіх обов'язкових видів навчальної роботи передбачених робочою програмою (лабораторних, модульного контролю та контрольної роботи). Мінімальна кількість балів необхідна для допуску до екзамену – 20.

Модуль за тематичним планом дисципліни та форма контролю		**Кількість балів**	
Змістовий модуль 1. Загальні положення нормативно-правового забезпечення інформаційної безпеки			
1	Повнота ведення конспектів занять (присутність на лекції+конспект – 1 бал за кожну лекцію)	0	5
2	Підготовленість до практичних занять. Рівень знань студента за темою практичного заняття (максимум - 2 бали за кожне пр.заняття)	0	10
3	Самостійна робота	0	5
4	Поточний модульний контроль	0	10
Змістовий модуль 2. Методологічні підходи до проектування технічних засобів захисту інформації			
1	Повнота ведення конспектів занять (присутність на лекції+конспект – 1 бал за кожну лекцію)	0	5
2	Підготовленість до практичних занять. Рівень знань студента за темою практичного заняття (максимум - 2 бали за кожне пр. заняття)	0	10
3	Самостійна робота	0	5
4	Поточний модульний контроль	0	10
Підсумкова оцінка		**0**	**60**
Залік		**0**	**40**
Всього		**0**	**100**

Шкала оцінювання: національна та ECTS

Критерії оцінювання	**Сума балів за всі види навчальної діяльності**	**Оцінка ECTS**	**Оцінка за національною шкалою**	
			для екзамену, КП	**для заліку**
Студент виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить	90 – 100	**A**	відмінно	зараховано

Критерії оцінювання	Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
			для екзамену, КП	для заліку
та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили, проводить наукові дослідження				
Студент вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв'язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна	82-89	**B**	добре	
Студент вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок	75-81	**C**		
Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих	66-74	**D**	задовільно	
Студент володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні	60-65	**E**		
Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу	0-59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання

7. Політики курсу.

7.1 Академічна доброчесність – самостійність виконання навчальних завдань та посилання на джерела у випадку використання напрацювань інших авторів. Види порушень академічної доброчесності – академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування, обман, хабарництво.

Відповідно до Положення про академічну доброчесність студентів та науково-педагогічних працівників Національного університету «Чернігівська політехніка» Затв. Вченою радою НУ «Чернігівська політехніка» 31 серпня 2020 р. протокол № 6 Введено в

дію наказом ректора від 31 серпня 2020 р. № 26 за порушення академічної доброчесності здобувачі освіти можуть мати наслідком: повторне проходження оцінювання (контрольна робота, іспит, залік тощо); повторне проходження відповідного освітнього компонента освітньої програми; відрахування із закладу освіти (крім осіб, які здобувають загальну середню освіту); позбавлення академічної стипендії; позбавлення наданих закладом освіти пільг з оплати навчання.

7.2 Політика дедлайнів – своєчасність здачі лабораторної роботи оцінюється в 0,5 бала за кожну лабораторну роботу. Своєчасність здачі РГР оцінюється в 2 бали. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом).

7.3 Політика перезарахування кредитів у випадку мобільності – перезарахування відбувається якщо назви навчальних дисциплін ідентичні або мають незначну стилістичну відмінність, але обсяги та змістова частина навчальних програм не відрізняються; кількість кредитів, відведена на вивчення навчальної дисципліни відрізняється менше, ніж на 25 %; форми підсумкового контролю з дисциплін однакові. При перезарахуванні дисципліни зберігається раніше здобута позитивна оцінка. Перескладання іспиту з дисципліни з метою підвищення оцінки, визначеної в документах виданих здобувачу вищої освіти за попереднім місцем навчання, не дозволяється. Перезарахування кредитів проводиться відповідно до Порядку визначення академічної різниці та перезарахування навчальних дисциплін у Національному університеті «Чернігівська політехніка» Затв. Вченою радою НУ «Чернігівська політехніка» 31 серпня 2020 р. протокол № 6 Введено в дію наказом ректора від 31 серпня 2020 р. № 26.

7.4 Політика щодо відвідування – відвідування занять є обов'язковим. При наявності поважних причин (хвороба, участь в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом) студенти можуть узгодити з викладачем індивідуальний графік навчання та здачі всіх видів навчальної роботи. Студенти можуть перескладати або відпрацьовувати пропущені заняття на консультаціях викладача чи у спеціально відведений викладачем для цього час.

7.5 Політика щодо правил поведінки на заняттях – активна участь у навчальному процесі, виконання необхідного мінімуму навчальної роботи, коректна поведінка щодо інших учасників навчального процесу, взаємоповага, використання мобільних пристроїв тільки для навчання.

7.6 Політика заохочень та стягнень. Результати навчальної, наукової та організаційної діяльності студентів за напрямами курсу їм можуть нараховуватися додаткові бали - до 10 балів, в залежності від вагомості досягнень студента. Види позанавчальної діяльності, за які студенти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, статті на науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

8. Рекомендована література та інформаційні джерела

1. Information Security Management — Specification With Guidance for Use : ISO/IEC 27001:2005. — Режим доступу: http://www.standards.-org/standards/listing/iso_27001 та ін.

2. Бурячок В.Л. Політика інформаційної безпеки : підручник / В. Л. Бурячок, Р. В. Грищук, В.О.Хорошко; за заг. ред. докт. техн. наук, проф. В. О. Хорошка. – К. : Задруга, 2014. – 222 с.

3. Державна служба спеціального зв'язку та захисту інформації України. – [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua

4. Доктрина інформаційної безпеки України: Указ Президента України від 25.02.2017 р. № 47/2017 // Офіційний вісник Президента України. – 2017. – № 5. – С. 15. – Ст. 102

5. Законодавче забезпечення інформаційної безпеки України / Фурашев В.М. // Інформація і право. – 2014. – № 1(10). – С. 59-67.

6. Законодавчі основи забезпечення інформаційної безпеки України: наукова доповідь / Пилипчук В.Г., Корж І.Ф., Петришин О.В., Савінова Н.А., Фурашев В.М. (За заг. ред. Пилипчука В.Г.) – К: НДІІП НАПрН України, 2014. – 60 с.

7. Марущак А. І. Інформаційне право: регулювання інформаційної діяльності : навчальний посібник / А. І. Марущак. – К. : Скіф, КНТ, 2008. – 344 с.

8. Офіційний портал Верховної Ради України [Електронний ресурс]. – Режим доступу: www.rada.gov.ua/

9. Правові засади протидії загрозам інформаційній безпеці та розвитку інформаційного законодавства України: Аналіт. Доповідь. / Пилипчук В.Г., Брижко В.М., Дзьобань О.П., Фурашев В.М. - К.: НДІІП НАПрН України, 2012. – 25 с.

10. Юдін О. Інформаційна безпека держави : [навч. посіб.] / О. Юдін, В. Богуш. – Х. : Консул, 2005. – 576 с.