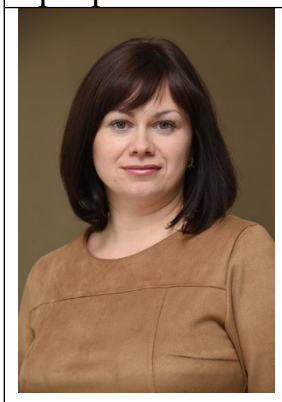
ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЕКОНОМІЧНИХ СИСТЕМАХ/
LEGAL PROVISION OF INFORMATION SECURITY IN ECONOMIC SYSTEM

СИЛАБУС/
SILABUS

ЗАТВЕРДЖЕНО
засіданням кафедри
(протокол №. 1
від «07» серпня 2024 р.)
завідувач кафедри
_____Олена КРИВОРУЧКО

Київ 2024

Назва освітньої компоненти	**ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЕКОНОМІЧНИХ СИСТЕМАХ/** LEGAL PROVISION OF INFORMATION SECURITY IN ECONOMIC SYSTEM
Спеціальність	125 «Кібербезпека та захист інформації»
Освітній ступінь	Другий (магістерський)
Освітньо-професійна програма	**БЕЗПЕКА СИСТЕМ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ В ЕКОНОМІЦІ**
	Лектор: **Ситниченко Олена** -доцент кафедри правового забезпечення безпеки бізнесу - кандидат юридичних наук, - доцент Резюме викладача: https://knute.edu.ua/blog/read/?pid=42323 е-пошта: o.sytnichenko@knute.edu.ua
Консультації	Кожен понеділок 4 пара в Teams
Програма освітньої компоненти	https://knute.edu.ua/blog/read/?pid=48216
ЗМІСТ ОСВІТНЬОЇ КОМПОНЕНТИ	
Тема 1. Теоретико-правові засади інформаційної безпеки та економічної безпеки України.	Основні підходи до визначення поняття «інформаційна безпека», «національна безпека», «економічна безпека». Співвідношення понять інформаційна безпека та національна безпека. Інформаційна безпека як інтегрована складова національної безпеки. Основоположні ідеї, засади інформаційної безпеки України. Правова сутність, мета і основні завдання економічної безпеки. Основи нормативно-правового регулювання питань національної безпеки в Україні. Характеристика основних положень Закону України «Про основи національної безпеки України». Законодавча та нормативно-правова база України у сфері інформаційної безпеки. Стратегія національної безпеки України, Стратегія кібербезпеки України тощо. Нормативно-правове регулювання економічної безпеки України. Система економічної інформації та її захист на основі законодавства України. Система економічної інформації та її захист. Основні принципи забезпечення захисту економічної інформації. Основні форми і способи забезпечення інформаційної безпеки. Учасники суспільних відносин в сфері інформаційної

	безпеки та економічної безпеки. Участь держави в процесі забезпечення інформаційної та економічної безпеки України. Об'єкти та суб'єкти інформаційної та економічної безпеки.
Тема 2. Компетенція держави в сфері інформаційної та економічної безпеки України. .	Поняття і структура інституціонального механізму забезпечення інформаційної безпеки. Пріоритет державної політики в інформаційній сфері. Стратегія інформаційної безпеки України. Державні суб'єкти, що впливають на процес формування і реалізації політики інформаційної безпеки України. Компетенція та розподіл функцій Президента України та основних органів державної влади – Верховної ради України та Кабінету Міністрів України в галузі інформаційної безпеки. Структура та компетенція Ради національної безпеки та оборони України. Інші органи державної влади, що виконують у рамках своєї діяльності окремі завдання щодо захисту інформаційної безпеки України: а) Рада національної безпеки і оборони України; б) Міністерство культури та інформаційної політики України; в) Служба безпеки України; г) Міністерство внутрішніх справ України; ґ) Державна служба спеціального зв'язку та захисту інформації України; д) Національна рада України з питань телебачення і радіомовлення; е) Державний комітет телебачення і радіомовлення України; ж) Національний банк України тощо. Поняття та сучасний стан економічної безпеки України. Основні виклики і загрози у сфері економічної безпеки України. Основні завдання державної політики у сфері фінансової безпеки. Організаційно-правове забезпечення економічної безпеки України. Повноваження вищих і центральних органів державної влади у сфері економічної безпеки.
Тема 3. Інформація в житті держави, суспільства, підприємств та людини. Загрози інформаційної безпеки в економічних системах.	Інформація як юридична категорія, підходи до її визначення. Характеристика інформаційної безпеки. Права і свободи людини в галузі інформації, які гарантовані Конституцією України. Класифікація інформації. Класифікація загроз. Сучасні загрози. Інформаційні ризики. Захист персональних даних як запорука особистої безпеки особи в умовах сучасних ризиків і загроз. Поняття, види і способи негативного інформаційного впливу на свідомість людини. Основні міжнародно-правові акти, якими визначаються права людини в інформаційній сфері. Значення інформації у підприємницькій діяльності. Загрози інформаційної безпеки на підприємстві. Витік інформації. Канали витоку інформації, їх види. Зміст завдань захисту інформації. Юридична відповідальність за порушення інформаційного

	законодавства.
Тема 4. Організаційно-правові основи захисту та обмеження обігу інформації в цілях забезпечення інформаційної безпеки в економічних системах.	Правове регулювання суспільного обігу інформації. Методи захисту інформації. Організаційні засоби захисту інформації. Поняття, ознаки та види режимів доступу до інформації. Правове регулювання обігу інформації, що становить державну таємницю. Юридична відповідальність за порушення державної таємниці та інших видів режиму доступу до інформації. Поняття та види конфіденційної інформації. Правове регулювання обігу інформації, що становить службову таємницю. Види та особливості правового регулювання обігу інформації, що становить професійну таємницю: а) адвокатська таємниця; б) лікарська таємниця; в) таємниця вчинення нотаріальних дій; г) таємниця страхування; д) банківська таємниця, є) комерційна таємниця.
Тема 5. Банківська таємниця та конфіденційність інформації банків.	Поняття та значення банківської таємниці згідно положень Закону України «Про банки і банківську діяльність». Способи збереження банківської таємниці шляхом: а) обмеження кола осіб, що мають доступ до інформації; б) організації спеціального діловодства з документами, що містять банківську таємницю; в) застосування технічних засобів для запобігання несанкціонованому доступу до електронних та інших носіїв інформації; г) застосування застережень щодо збереження банківської таємниці та відповідальності за її розголошення у договорах і угодах між банком і клієнтом. Перелік законодавчо передбачених вимог, що висуваються для розкриття банківської таємниці. Відповідальність за розкриття банківської таємниці
Тема: 6. Правові засади безпеки інформаційної інфраструктури. Кібербезпека.	Правові засади забезпечення кібербезпеки України. Державні стандарти інформаційної безпеки та кібербезпеки. Міжнародні стандарти в галузі інформаційної безпеки та кібербезпеки. Глобальний індекс кіберспроможності. Поняття та напрями безпеки інформаційної інфраструктури. Інформаційна безпека та мережа Інтернет. Глобальний та локальний інформаційний простір та їх характеристики. Захист інформації в інформаційних системах. Криптографічний захист інформації. Технічний захист інформації. Правова система забезпечення захисту критичної інформаційної інфраструктури. Захист автоматизованих баз даних. Визначення поняття «кібератака» та «кібербезпека». Застосування термінів «інформаційна безпека» та «кібербезпека». Характеристика кіберзлочинності. Стан кіберзлочинності в Україні. Боротьба з кіберзлочинами.

Тема 7. Організаційне забезпечення захисту інформації та економічної безпеки підприємства.	Основні правові принципи забезпечення захисту інформації в економічній системі підприємства. Сутності та складова системи забезпечення економічної безпеки. Джерела зовнішніх та внутрішніх загроз на підприємстві. Персонал як одна із загроз розголошення та втрати інформації підприємства з обмеженим доступом. Особливості прийняття працівників на роботу та звільнення з роботи, пов'язаної з доступом до таємниць підприємства. Доступ персоналу до документів і матеріалів, які містять інформацію з обмеженим доступом. Порядок доступу співробітників до конфіденційної інформації. Поняття і принципи організації конфіденційного документообігу. Дозвільна система доступу до конфіденційних документів. Структура підрозділів, що здійснюють захист інформації. Організація діяльності служби інформаційної безпеки підприємства. Організація виконання конфіденційних документів. Основні юридичні форми і способи забезпечення інформаційної безпеки економічної системи підприємства.
Тема 8. Інформаційні ресурси підприємства, банку. Організація інформаційно-аналітичної роботи на підприємстві, банку.	Історичний погляд на появу інформаційних ресурсів. Категорія «інформаційні ресурси» в праві. Роль та місце інформаційних ресурсів на підприємстві, банку. Властивості інформаційних ресурсів. Функції інформаційних ресурсів. Зміст, принципи, завдання інформаційно-аналітичної роботи та структура процесу її організації. Інформаційні канали як джерела отримання інформації. Основні заходи інформаційно-аналітичної роботи банків: інформаційний моніторинг; аудит.
Тема 9. Види юридичної відповідальності за правопорушення в інформаційній сфері економічних систем.	Поняття та види інформаційних правопорушень. Підстави юридичної відповідальності за вчинення правопорушень в інформаційній сфері економічних систем. Характеристика окремих видів інформаційно-правової відповідальності. Адміністративно-правовий захист інформації. Адміністративна відповідальність за інформаційні правопорушення. Поняття кіберзлочинності та кримінальна відповідальність. Юридична відповідальність за кримінальні правопорушення в інформаційній сфері економічних систем. Основні положення Конвенції Ради Європи «Про кіберзлочинність» як базового міжнародного нормативно-правового акту, що регулює суспільні відносини у сфері протидії кіберзлочинам. Цивільно-правова відповідальність за інформаційні правопорушення. Інформаційний делікт. Правовий захист об'єктів економічних систем підприємств, установ та організацій від протиправних посягань на основі

	діючого законодавства України.
Тема 10. Правове забезпечення інформаційної безпеки та інших складових економічної безпеки України.	Поняття та сучасний стан соціальної, продовольчої, енергетичної та демографічної безпеки України. Основні виклики і загрози у сфері соціальної, продовольчої, енергетичної та демографічної безпеки України. Основні завдання державної політики у сфері соціальної, продовольчої, енергетичної та демографічної безпеки. Організаційно-правове забезпечення соціальної, продовольчої, енергетичної та демографічної безпеки України. Повноваження вищих і центральних органів державної влади у сфері соціальної, продовольчої, енергетичної та демографічної безпеки. Компетенція Ради національної безпеки і оборони України, Бюро економічної безпеки України, Державного бюро розслідувань із забезпечення соціальної, продовольчої, енергетичної та демографічної безпеки України. Застосування механізму економічних санкцій до країни-агресорки під час широкомасштабної агресії рф проти України.

СПИСОК ОСНОВНИХ РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Остроухов В.В., Присяжнюк М. М., Фармагей О. І., Чеховська М. М. Інформаційна безпека : підруч. [за загал. ред. В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська]. – Видавництво Ліра-К, 2021. – 412 с.
2. Бобало Ю.Я, Горбатий І.В, Кіселичник М.Д., Бондарєв А.П, Войтусік С.С. Інформаційна безпека: навч.посібник [за заг.ред. Ю.Я. Бобала]. – Видавництво Львівська політехніка – 2019. – 580 с.
3. Гребенюк А.М. Основи управління інформаційною безпекою : навч. посібник [за заг.ред. А.М. Гребенюк, Л.В. Рибальченко]. – Видавництво Дніпро : Дніпроп. держ. Ун-т внутріш. справ, 2020. – 144 с.
4. *Іванюта Т.М., Заічковський А.О. Економічна безпека підприємництва: навчальний посібник [за заг.ред. Т.М. Іванюта, А.О. Заічковський]. – Видавництво – Київ: Центр учбової літератури, 2018. – 256 с.*
5. Лужецький В.А., Войтович О.П., Дудатьєв А.В. Інформаційна безпека : навч. посіб. -Вінниця: УНІВЕРСУМ-Вінниця, 2015. – 239 с

РЕЗУЛЬТАТИ ВИВЧЕННЯ ОСВІТНЬОЇ КОМПОНЕНТИ

Дисципліна забезпечує оволодіння здобувачами вищої освіти загальними та фаховими компетентностями і досягнення ними програмних результатів навчання:

КЗ-01.	Здатність застосовувати знання у практичних ситуаціях.
КЗ-02.	Здатність проводити дослідження на відповідному рівні.

КЗ-05.	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КЗ-06.	*Здатність діяти соціально відповідально та громадсько свідомо.*
КЗ-07.	*Здатність до адаптації та дії у новій ситуації.*
КЗ-08.	*Здатність до вибору стратегії спілкування, працювати в команді.*
КФ-01.	Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
КФ-02.	Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
КФ-03.	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
КФ-04.	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
КФ-10.	Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
КФ-12.	*Здатність виконувати обов’язки внутрішнього консультанта і радника у своїй експертній області.*
РН -01	Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН -05	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН 06	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН-07	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач про-

	фесійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН-12	Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН-14	Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН-17	Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН-22	Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН-25	*Виконувати обов'язки внутрішнього консультанта/ радника в технічній сфері та галузі авторського права щодо електронних носіїв інформації.*
РН-26	*Комунікувати з керівниками різних рівнів (міжособистісне спілкування, доступність, уміння ефективно сприймати мову виступаючих, відповідно до аудиторії коректувати стиль і мову виступу).*

ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ ОСВІТИ

Сума балів, накопичених здобувачем вищої освіти за виконання всіх видів поточних навчальних завдань (робіт) на лабораторних/практичних заняттях, свідчить про ступінь оволодіння ним програмою освітньої компоненти на конкретному етапі її вивчення. Протягом семестру здобувачі освіти можуть набрати від 0 до 100 балів, що переводяться у національну шкалу оцінювання і відповідно у шкалу ЄКТС. Кількість балів відповідає певному рівню засвоєння дисципліни

Довідник з розподілу оцінок ДТЕУ (Шкала ЄКТС):

Бали ДТЕУ	Відсоток балів відносно загальної кількості одержаних прохідних балів	Кумулятивний відсоток отриманих прохідних балів
90-100	20	20
82-89	10	зо
75-81	20	50
69-74	10	60
60-68	40	100

Розподіл балів за видами робіт:

Вид роботи	**Бали**	**Вид роботи**	**Бали**
Практична робота 1	4	Самостійна робота 1	2
Практична робота 2	4	Самостійна робота 2	2
Практична робота 3	4	Самостійна робота 3	3
Практична робота 4	4	Самостійна робота 4	3
Практична робота 5	4	Самостійна робота 5	3
Практична робота 6	3	Самостійна робота 6	3
Практична робота 7	4	Самостійна робота 7	3
Практична робота 8	4	Самостійна робота 8	3
Практична робота 9	5	Самостійна робота 9	3
Практична робота 10	5	Самостійна робота 10	3
Додаткові бали + Захист проєкту	20	Наукова робота	10

Вимоги до критеріїв оцінювання самостійної роботи студента (оцінювання одного завдання у відсотковому еквіваленті)

40%	Детальний розгляд сутності та вмісту основних джерел. Подання фактів, ідей і результатів досліджень у логічній послідовності. Правильно проаналізовано поточний стан дослідження проблеми та зроблено огляд перспектив подальшого розвитку даного питання.
40%	Обґрунтованість аргументів, підтвердження особистого ставлення, пропозиції стосовно вирішення завдання, встановлення напрямків аналізу.
20%	Оформлення звіту у відповідності вимог

Критерії оцінювання самостійної роботи студента (оцінювання одного завдання у відсотковому еквіваленті)

100%	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та лабораторних завдань, використовуючи при цьому обов’язкову та додаткову літературу. Правильно вирішив усі тестові завдання.
80%	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та лабораторних завдань, використовуючи при цьому обов’язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві

	неточності та незначні помилки. Правильно вирішив більшість тестових завдань
60%	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
40%	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та лабораторних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань.
20%	Частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.
0%	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.

ОСНОВНІ ПОЛОЖЕННЯ, ЩО РЕГЛАМЕНТУЮТЬ ОСВІТНІЙ ПРОЦЕС

діючі положення	https://knute.edu.ua/blog/read/?pid=44402
нормативно-правова база організації освітнього процесу	https://knute.edu.ua/blog/read/?pid=7330&uk
студенту	https://knute.edu.ua/#forstudent

НЕФОРМАЛЬНА ОСВІТА

Рекомендовані сертифікаційні програми, курси, посібники користувача

European Union Agency for Cybersecurity (Агентство Європейського Союзу з питань кібербезпеки)	https://www.enisa.europa.eu
The EU Cyberdiplomacy Toolbox	https://www.cyber-diplomacy-toolbox.com/
MS AZURE	https://learn.microsoft.com/uk-ua/training/azure/
Cloud Native Computing Foundation	https://www.cncf.io/
Isaca	https://www.isaca.org/training-and-events
CSA (Cloud security alliance)	https://cloudsecurityalliance.org/research/artifacts

ПОЛІТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ:

Відвідування лекційних та лабораторних занять: відвідування	Відвідування лекційних та лабораторних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому конкурсі тощо за попередньою домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).
Відпрацювання пропущених занять:	відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лекційне заняття має бути відпрацьоване до наступної лекції на консультації викладача з використанням ПЗ 365 Office Teams. Відпрацювання лекційного матеріалу передбачає вивчення пропущеного теоретичного матеріалу та складання тесту за цим матеріалом. Лабораторне заняття відпрацьовується під час консультації викладача (розклад консультацій на сайті).
Правила поведінки під час занять	обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчально матеріалу ознайомившись з ним напередодні (навчальний матеріал надається викладачем). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки практичних завдань в процесі заняття. Задля зручності, дозволяється використання ноутбуків та інших електронних пристроїв під час навчання в комп'ютерних аудиторіях (за взаємною згодою всіх учасників освітнього процесу)
Політика академічної доброчесності ДТЕУ	https://knute.edu.ua/blog/read/?pid=38987&uk