МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Юридичний факультет

Кафедра кримінального правосуддя та правоохоронної діяльності

СИЛАБУС
вибіркового освітнього компонента
КІБЕРГІГІЄНА

підготовки бакалавра

Луцьк - 2025

Силабус вибіркового освітнього компонента «Кібергігієна» підготовки бакалавра

Розробник: Дем’як Павло Юрійович, викладач кафедри кримінального правосуддя та правоохоронної діяльності юридичного факультету Волинського національного університету імені Лесі Українки

Погоджено

Гарант освітньо-професійної програми (Кравчук В.М.)

Силабус вибіркового освітнього компонента затверджено на засіданні кафедри кримінального правосуддя та правоохоронної діяльності

протокол № 1 від «28» серпня 2025 р.

Завідувач кафедри: Фідря Ю.О.

1. Опис освітнього компонента

Денна форма навчання

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна програма, освітній рівень</th><th>Характеристика освітнього компонента</th></tr>
<tr><td rowspan="2">Денна (очна) форма навчання</td><td rowspan="5">Галузь знань
D Бізнес, адміністрування та право,
Спеціальність Д8
Право,
освітньо-професійна програма Право.
освітній рівень:
перший (бакалаврський)</td><td>Вибірковий</td></tr>
<tr><td>Рік навчання 2-й</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів 150/5</td><td>Семестр 3-ий</td></tr>
<tr><td>Лекції 24 год.</td></tr>
<tr><td>Практичні (семінарські) 26 год.</td></tr>
<tr><td rowspan="2">ІНДЗ: немає</td><td>Самостійна робота 90 год.</td></tr>
<tr><td>Консультації 10 год.</td></tr>
<tr><td>Форма контролю: залік</td></tr>
<tr><td colspan="2">Мова навчання Українська</td><td></td></tr>
</table>

Заочна форма навчання

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна програма, освітній рівень</th><th>Характеристика освітнього компонента</th></tr>
<tr><td rowspan="2">Заочна форма навчання</td><td rowspan="5">Галузь знань
D Бізнес, адміністрування та право,
Спеціальність Д8
Право,
освітньо-професійна програма Право.</td><td>Вибірковий</td></tr>
<tr><td>Рік навчання 2-й</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів 150/5</td><td>Семестр 3-ий</td></tr>
<tr><td>Лекції 6 год.</td></tr>
<tr><td>Практичні (семінарські) 8 год.</td></tr>
<tr><td rowspan="2">ІНДЗ: немає</td><td>Самостійна робота 118 год.</td></tr>
<tr><td>Консультації 18 год.</td></tr>
</table>

	освітній рівень: перший (бакалаврський)	**Форма контролю:** залік
Мова навчання Українська		

2. Інформація про викладача

ПІБ: Дем’як Павло Юрійович

Посада: викладач кафедри кримінального правосуддя та правоохоронної діяльності

Контактна інформація: +380995171901, pavlodemyak@ukr.net

ІІ. Опис освітнього компонента

1. Анотація освітнього компонента

Програма освітнього компонента спрямована на формування у здобувачів освіти базових знань механізму безпеки при роботі з комп'ютером, основних засад кібергігієни на робочому місці та в повсякденному житті, використання сучасних комп'ютерно-інформаційних технологій, а також забезпечити формування інформаційної культури та набуття практичних навичок для застосування у майбутній професії.

2. Пререквізитами

Вивчення нормативного освітнього компонента передбачає наявність базових знань з інформатики, галузевих професійних наук, а також навиків у тлумаченні та реалізації права.

3. Мета і завдання освітнього компонента

Мета цього навчального освітнього компонента полягає в тому, щоб розвивати у студентів вміння, які сприяють конкретному та послідовному мисленню, здатність висловлювати свої власні думки, критичне мислення, роботу з різноманітними джерелами та фактичним матеріалом, а також вміння чітко й точно висловлювати свої погляди, аргументувати їх і брати участь в обґрунтованих дискусіях.

Програма цього освітнього компонента сформує необхідні знання щодо правильного поводження з інформацією у кіберсфері та безпечної роботи із компютерної технікою в професійній діяльності. Слухачі дізнаються про основні загрози в сучасному інформаційному просторі, наслідки атак зловмисників та кібершахраїв.

Набуті у ході вивчення освітнього компонента навички підвищать конкурентоспроможність молодих фахівців на ринку праці.

Для досягнення поставленої мети передбачені такі основні завдання:

- знання основних положень, термінів та заходів, що стосуються кібергігієни на робочому місці;
- знання нормативно-правової бази у сфері кібербезпеки;
- уміння оцінювати загрози та вживати заходів реагування на робочому місці;
- уміння безпечно поводитись у кіберпросторі;
- знати методи якими нападники проникають в комп'ютерну систему: соціальна інженерія, злам паролю, фішинг, спуфінг та інше.

4. Результати навчання (Компетентності)

Загальні компетентності (ЗК): здатність застосовувати знання у практичних ситуаціях (ЗК 2); знання та розуміння предметної області та розуміння професійної діяльності (ЗК 3); здатність використовувати інформаційні та телекомунікаційні технології (ЗК6); здатність вчитися і оволодівати сучасними знаннями (ЗК7).

Спеціальні компетентності (СК): здатність застосовувати правові принципи та доктрини (СК8); здатність використовувати різноманітні інформаційні джерела для повного та всебічного встановлення певних обставин (СК10); здатність визначати належні та прийнятні для юридичного аналізу факти (СК 11); здатність до критичного та системного аналізу правових явищ (СК 13);

здатність до консультування з правових питань, зокрема, можливих способів захисту прав та інтересів клієнтів, відповідно до вимог професійної етики, належного дотримання норм щодо не розголошення персональних даних та конфіденційної інформації (СК 14); здатність до логічного, критичного і системного аналізу документів, розуміння їх правового характеру і значення (СК 16).

Результати навчання (РН): визначати переконливість аргументів у процесі оцінки заздалегідь невідомих умов та обставин (РН 1), проводити збір і інтегрований аналіз матеріалів з різних джерел (РН 3), давати короткий правовий висновок щодо окремих фактичних обставин (даних) з достатньою обґрунтованістю (РН 5), самостійно визначати ті обставини, у з’ясуванні яких потрібна допомога, і діяти відповідно до отриманих рекомендацій (РН 9), використовувати статистичну інформацію, отриману з першоджерел та вторинних джерел для правничої діяльності (РН 14), вільно використовувати для правничої діяльності доступні інформаційні технології і бази даних (РН 15), використовувати комп’ютерні програми, необхідні у правничій діяльності (РН 16), виокремлювати і аналізувати юридично значущі факти і робити обґрунтовані правові висновки (РН 20).

5. Структура освітнього компонента

Денна форма навчання

Назви змістових модулів і тем	Усього	Лек.	Практ.	Лабор.	Сам. роб.	Конс.	Форма контролю / Бали
Тема 1. Кіберпростір, кібербезпека та інформаційна безпека.		2	2	-	11	1	ДС+ДБ+УО
Тема 2. Забезпечення захисту особистої інформації, зменшення ризику витоку персональних даних.		4	4	-	11	1	ДС+УО+РЗ/К+УО
Тема 3. Захист пристроїв та гаджетів.		4	6	-	11	2	ДС+УО+РЗ/К+УО
Тема 4. Комп'ютерна вірусологія.		4	4	-	11	1	ДС+УО+ДЗ/К+УО
Тема 5. Практичні поради для захисту пристроїв від дистанційних атак		2	2	-	11	**1**	ДС+УО+ДЗ/К+УО
Тема 6. Соціотехнічна безпека.		2	4	-	11	2	ДС+УО+РЗ/К+УО
Тема 7. Системи захисту інформації.		4	2	-	12	1	ДС+УО+РЗ/К+УО
Тема 8. Кібергігієна: правова база, ресурси та інструменти у професійній діяльності.		2	2	-	12	1	ДС+ДБ+Т+УО
Всього годин/Балів	**56**	**24**	**26**	**0**	**90**	**10**	

Заочна форма навчання

Назви змістових модулів і тем	Усього	Лек.	Практ.	Лабор.	Сам. роб.	Конс.	Форма контролю / Бали
Тема 1. Кіберпростір, кібербезпека та інформаційна безпека.		2		-	16	1	ДС+ДБ+УО
Тема 2. Забезпечення захисту особистої інформації, зменшення ризику витоку персональних даних.		2	2	-	16	1	ДС+УО+РЗ/К+УО
Тема 3. Захист пристроїв та гаджетів.			2	-	16	2	ДС+УО+РЗ/К+УО
Тема 4. Комп'ютерна вірусологія.		2	2	-	16	1	ДС+УО+ДЗ/К+УО

Тема 5. Практичні поради для захисту пристроїв від дистанційних атак				-	16	**1**	ДС+УО+ ДЗ/К+УО
Тема 6. Соціотехнічна безпека.				-	14	2	ДС+УО+ РЗ/К+УО
Тема 7. Системи захисту інформації.				-	12	1	ДС+УО+ РЗ/К+УО
Тема 8. Кібергігієна: правова база, ресурси та інструменти у професійній діяльності.			2	-	12	1	ДС+ДБ+ Т+УО
Всього годин/Балів	**56**	**6**	**8**	**0**	**118**	**10**	

*Методи контролю: ДС - дискусія, ДБ - дебати, Т - тести, РЗ/К - розв’язування задач/кейсів, УО - усне опитування.

**Порядок нарахування балів за поточний контроль див. у розділі «Політика оцінювання».

6. Інформаційний обсяг ОК

Тема 1. Кіберпростір, кібербезпека та інформаційна безпека. Поняття, визначення та тренди розвитку кіберпростору та кібергігієни. Історичний розвиток та складові безпеки в кіберпросторі. Інформаційна безпека держави, організації, особистості. Інформація як об'єкт захисту. Тріада кібербезпеки - конфіденційність, цілісність, доступність. Вступ та знайомство з основними визначеннями, інформаційними ресурсами. Властивості інформації як об'єкта захисту. Оцінка рівнів захищеності.

Тема 2. Забезпечення захисту особистої інформації, зменшення ризику витоку персональних даних. Захист облікових даних. Облікові записи та паролі доступу. Види атак на облікові записи. Робота з поштою, додатками та сервісами. Характеристика сучасних кібератак. Оцінка ризиків цифрової безпеки. Надійні паролі, двофакторна автентифікація. Захист від фішингу. Контроль сесій, сповіщення про вхід. Переадресація в пошті.

Тема 3. Захист пристроїв та гаджетів. Захист пристроїв від дистанційних атак. Легальне програмне забезпечення. Оновлення програмного забезпечення та антивірусу. Захист пристроїв від стороннього фізичного доступу. Захист комунікацій (голос, чат, email, файли, відеодзвінки - від провайдера, хакерів, корпорацій). Робота в мережах. VPN-з'єднання. Небезпеки комунікації з допомогою мобільного зв'язку (голос, SMS, мобільний інтернет, 2G/3G/4G/5G). Анонімність в мережі. Захист пристроїв від дистанційних атак. Використання ліцензійного програмного забезпечення. Антивіруси та їхні додаткові компоненти. Нешифроване та шифроване з'єднання з сайтами. Особливості комунікації за допомогою стільникового зв'язку. Безпечність використання месенджерів. Робота в публічних місцях. Підготовка пристроїв до роботи в умовах високих ризиків.

Тема 4. Комп’ютерна вірусологія. Загальні поняття про компютерної віруси. Класифікація комп'ютерних вірусів. Типи шкідливого програмного забезпечення. Шляхи розповсюдження шкідливого програмного забезпечення. Макровіруси та мережеві віруси. Файлові та завантажувальні віруси. Викрадачі інформації keylogger. Троянські програми віддаленого доступу. Майнери. Програми-вимагачі. ШПЗ для

знищення інформації. Рекламне шкідливе програмне забезпечення.

Тема 5. Практичні поради для захисту пристроїв від дистанційних атак на базі: OS Windows, MacOS, Linux. Практичні поради для захисту мобільних пристроїв на базі Android, iOS. Захист роутера від дистанційних атак (TP-Link, ASUS, MikroTik, Keenetic, Cisco).

Тема 6. Соціотехнічна безпека. Поняття соціальної інженерії. Методи та види атак соціальної інженерії. Претекстінг (pretexting). Тейлгейтінг (tailgating). Послуга за послугу (quid pro quo).

Тема 7. Системи захисту інформації. Технології захисту інформації на основі програмного забезпечення. Ризики втрати важливої інформації. Практичні рекомендації щодо захисту цифрових даних.

Тема 8. Кібергігієна: правова база, ресурси та інструменти у професійній діяльності. Правові аспекти та політики цифрової безпеки. Політика України та держав світу в галузі кібергігієни. Центри моніторингу та інформування про кіберзагрози. НКЦК. CERT-UA. MISP-UA Знайомство з державними документами та організаціями з кібернетичної безпеки. Знайомство з системою управління кібербезпекою на рівні держави. Досвід передових країн.

7. Завдання для самостійного опрацювання.

Самостійна робота передбачає опрацювання теоретичних основ лекційного матеріалу по кожній темі та виконання завдань і оцінюється викладачем індивідуально відповідно до пікали оцінювання.

8. Методи навчання.

При вивченні дисципліни використовуються:

Дидактичні методи - лекції з використанням мультимедійних презентацій.

Практичні методи: практичні заняття з використанням прикладного програмного забезпечення.

Метод самостійного навчання.

Активні методи: експрес опитування, тестування.

Словесні методи навчання: лекції, консультації.

9. Технічне й програмне забезпечення /обладнання.

Комп’ютери, компоненти програмного забезпечення MS Office 365 (Teams, PowerPoint, Word), вільне програмне забезпечення (GNU General Public License), електронне освітнє середовище - Віртуальний університет (на базі платформи Moodle).

ІІ.Політика оцінювання

Політика викладача щодо студента

Формуючи лекційний матеріал і практичні завдання, викладач створює умови для найбільш ефективного засвоєння здобувачем освіти знань в рамках пропонованого освітнього компонента. Досягненню відповідної мети слугує, зокрема визначення тих питань, що за рівнем складності можуть бути вивчені студентом в рамках самопідготовки.

При цьому в ході викладення освітнього компонента викладач використовує сучасні наукові методи, спрямовані в тому числі на розвиток у здобувачів освіти критичного мислення і вміння самостійно аналізувати обставини правової реальності та давати їм оцінку з точки зору положень чинного законодавства України і норм міжнародного права.

Відвідування лекційних і практичних занять здобувачем освіти покликане

забезпечити отримання ним концентрованих знань, що досягається у тому числі безпосередньою участю в обговоренні відповідної тематики, а також зверненням до викладача із запитаннями з метою конкретизації тих чи інших аспектів предмету розгляду. Поряд із цим, для забезпечення освітнього компонента викладач використовує сучасні технології, зокрема хмарні сервіси і освітні платформи чим створює можливості для самостійного ефективного засвоєння здобувачем освіти пропонованого матеріалу у межах елементів структури освітнього компонента. У зв'язку з цим, якщо інше не встановлено положеннями нормативно-правових документів Університету, здобувач освіти, який пропустив лекційне або практичне заняття, може самостійно опрацювати відповідний матеріал і пройти контроль знань з використанням відповідних електронних сервісів або ж пройти контроль знань на одному з практичних аудиторних занять. Також у разі необхідності здобувач освіти може відвідати консультацію з конкретної теми для заповнення прогалин у знаннях.

Політика щодо академічної доброчесності

Дотримання академічної доброчесності педагогічними, науково- педагогічними та науковими працівниками передбачає:

- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про методики і результати досліджень, джерела використаної інформації та власну педагогічну (науково-педагогічну, творчу) діяльність;
- контроль за дотриманням академічної доброчесності здобувачами освіти;
- об’єктивне оцінювання результатів навчання.

Дотримання академічної доброчесності здобувачами освіти передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:

академічний плагіат - оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;

самоплагіат - оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;

фабрикація - вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;

фальсифікація - свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;

списування - виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання;

обман - надання завідомо неправдивої інформації щодо власної освітньої (наукової, творчої) діяльності чи організації освітнього процесу; формами обману є, зокрема, академічний плагіат, самоплагіат, фабрикація, фальсифікація та списування;

хабарництво - надання (отримання) учасником освітнього процесу чи пропозиція щодо надання (отримання) коштів, майна, послуг, пільг чи будь-яких інших благ матеріального або нематеріального характеру з метою отримання неправомірної переваги в освітньому процесі;

необ'єктивне оцінювання - свідоме завищення або заниження оцінки результатів навчання здобувачів освіти;

надання здобувачам освіти під час проходження ними оцінювання результатів навчання допомоги чи створення перешкод, не передбачених умовами та/або процедурами проходження такого оцінювання;

вплив у будь-якій формі (прохання, умовляння, вказівка, погроза, примушування тощо) на педагогічного (науково-педагогічного) працівника з метою здійснення ним необ'єктивного оцінювання результатів навчання.

Політика щодо дедлайнів та перескладання

Поточний контроль за темами освітнього компонента здійснюється в рамках практичних занять, що проводяться згідно з розкладом.

Здобувач освіти має право повторно скласти поточний контроль за темою лише один раз.

Якщо тема передбачає надання здобувачем освіти усної відповіді щодо питань плану теми, а також вирішення юридичної задачі, здобувач освіти має право повторно скласти ту частину (ті частини) завдань, за які ним одержані бали нижче максимальних.

Зараховується найбільший результат, одержаний здобувачем освіти за результатами складання відповідної частини завдань або їх повторного складання.

Ліквідація академічної заборгованості здійснюється централізовано для всіх здобувачів освіти у визначений викладачем час до дати, встановленої для повторного проведення іспиту («перша, друга та третя відомості»).

III. Підсумковий контроль

Оцінювання знань здобувачів освіти здійснюється під час поточного контролю за результатами виконання тих видів робіт, які передбачені силабусом освітнього компонента в діапазоні від 0 до 100 балів. Мінімальна позитивна кількість балів, як правило, - 60.

Здобувач освіти може додатково скласти на консультаціях із викладачем ті теми, які він пропустив протягом семестру (з поважних причин), таким чином покращивши свій результат рівно на ту суму балів, яку було виділено на пропущені теми. У дату складання заліку викладач записує у відомість суму поточних балів, які здобувач освіти набрав під час поточної роботи (шкала від 0 до 100 балів).

У випадку, якщо здобувач освіти набрав менше ніж 60 балів, він складає залік під час ліквідації академічної заборгованості. У цьому випадку бали, набрані під час поточного оцінювання, анулюються. Максимальна кількість балів під час ліквідації академічної заборгованості з заліку, як правило, - 100.

Ліквідація академічної заборгованості здійснюється на платформі moodle шляхом складання тесту.

VI. Шкала оцінювання

Оцінка в балах	**Лінгвістична оцінка**	**Оцінка за шкалою ECTS**	
		оцінка	**пояснення**
90-100	Відмінно	A	відмінне виконання
82-89	Дуже добре	B	вище середнього рівня
75-81	Добре	C	загалом хороша робота
67-74	Задовільно	D	непогано
60-66	Достатньо	E	виконання відповідає мінімальним критеріям
1-59	Незадовільно	Fx	Необхідне перескладання

БАЛИ ЗАРАХУВАННЯ ФОРМАЛЬНОЇ, НЕФОРМАЛЬНОЇ ТА ІНФОРМАЛЬНОЇ ОСВІТИ

Види студентської наукової та практичної активності	Кількість балів
Публікація наукової статті в періодичному виданні студентських наукових праць	10
Виступ на Міжнародній, Всеукраїнській студентській науково- практичній конференції з публікацією тез доповіді	5
Участь у ІІ етапі Всеукраїнського конкурсу студентських олімпіад	до 20
Участь у ІІ етапі Всеукраїнського конкурсу наукових робіт	до 20
Участь у всеукраїнських та міжнародних змаганнях Moot Court	до 20
Участь у роботі юридичної клініки “Ad ASTRA” згідно реєстру КЛІНІПИСТІВ.	до 10
Участь у правопросвітніх заходах організованих громадськими організаціями в межах національних та міжнародних грантів.	до 5
Проходження курсів, тренінгів, воркшопів та інших видів неформальної освіти в межах тематики освітнього компонента	до 10

VII. Рекомендована література та інтернет-ресурси

1. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. - [Видання друге, перероб. та доп.]. - Одеса.: ОНАЗ ім. О.С. Попова, 2019. - 320 с. ISBN 978-617-582-069-8

2. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ратехн. наук, професора В. Б. Толубка - К.: ДУТ, 2015.- 288 с.

3. Безпека інформаційних систем: навч. посіб. / В. І. Пашорін, Ю. В. Костюк. - Київ: Держ. торг.-екон. ун-т, 2022. - 376 с. 4. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. - 144 с.

Інтернет ресурси:

1. Основи кібергігієни. Як держслужбовцям захиститися від хакерських атак - https ://osvita. diia. gov, па/courses/cyber-hygiene

2. Цифрова безпека для громадських організацій в умовах війни - https ://prometheus. org.ua/course/course-vl :Prometheus+DSPO 101 +2023_T 1 ?utm _source=sendy&utm_medium=email&utm_canipaign=email-aprildigest23-digital securit