

Силабус ВК Технології захисту інформації

Назва дисципліни:	Технології захисту інформації
Рівень вищої освіти:	перший (бакалаврський)
Сторінка курсу в Moodle:	https://dl2022.khadi-kh.com/course/view.php?id=6689
Обсяг освітнього компоненту	4 кредита (120 годин)
Форма підсумкового контролю	Залік
Консультації:	за графіком
Назва кафедри:	Кафедра кібербезпеки
Мова викладання:	українська
Керівник курсу:	Пікрасов Михайло Михайлович
Контактний телефон:	0679449675
E-mail:	mpiks77@gmail.com

Короткий зміст освітнього компоненту:

Метою є отримання компетентностей та навичок щодо обґрунтування застосування механізмів захисту та оцінки рівня захищеності інформаційно-комунікаційних систем і технологій від несанкціонованого доступу до ресурсів.

Предмет: необхідність комплексних систем захисту інформації. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній сфері.

Основними завданнями вивчення навчальної дисципліни є збереження цінності інформаційних ресурсів для їх власника. Збереження певних технологій їх створення, оброблення, зберігання, пошуку та надання користувачам. Вивчення та засвоєння основних принципів проектування та побудови захищених систем і оцінки їх надійності.

Компетентності, яких набуває здобувач:

Загальні компетентності:

- Здатність формулювати та забезпечувати вимоги щодо якості програмного забезпечення у відповідності з вимогами замовника, технічним завданням та стандартами;
- Здатність до виявлення, генерування, дослідження та вирішення проблем за професійним спрямуванням. фахові компетентності.

Спеціальні компетентності:

- Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки);
- Здатність до забезпечення захисту інформації, що обробляється в інформаційно комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації.

Результати навчання:

- Знати та вміти використовувати методи та засоби збору, формулювання та аналізу вимог до програмного забезпечення.
- Застосовувати на практиці інструментальні програмні засоби доменного аналізу, проектування, тестування, візуалізації, вимірювань та документування програмного забезпечення.
- Знати підходи щодо оцінки та забезпечення якості програмного забезпечення.
- Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

Тематичний план

№ теми	Назва тем (ЛК, ЛР, ПР, СЗ, СР)	Кільк. год
1	ЛК1 Складові «Інформаційної безпеки», Основні поняття та задачі криптології	2
	ПР1 Класичний шифр простої заміни та його криптоаналіз. Біграмний шифр. Дослідження шифру Цезаря.	2
	СР1 Види шифрів	10
2	ЛК2. Безпека в інформаційних мережах. Фізична безпека. Загальна характеристика систем захисту в інформаційних мережах	2
	ПР2 Аналіз ризиків та основні принципи забезпечення інформаційної безпеки.	2
	СР2 Телекомунікації та віддалений доступ. Резервне копіювання. Адміністрування інформаційних систем	12
3	ЛК3 Класичні шифри та їх криптоаналіз	2
	ПР3 Класичний шифр поліалфавітної заміни та його криптоаналіз. Шифр Віженера.	2
	СР3 Моноалфавітний шифр	10
4	ЛК4 Криптографічна стійкість шифрів	2
	ПР4 Моделювання процесів шифрування за допомогою операції XOR.	2
	СР4 Типи атак на криптосистеми	12
5	ЛК5 Система захисту комп'ютера за допомогою BIOS	2
	ПР5 Налаштування особистого захисту ПК.	2
	СР5 Види BIOS	10
6	ЛК6 Удосконалений стандарт шифрування AES	2
	ПР6 Алгоритм AES	2
	СР6 Режими виконання блокових шифрів	12
7	ЛК7 Національний стандарт шифрування ДСТУ 7624:2014	2
	ПР7 Режими роботи «Калина»	2
	СР7 «Калина» vs AES	10
8	ЛК8 Основні положення криптографії з відкритим ключем	2
	ПР8 Алгоритм рюкзака (криптосистема Меркла-Хелмана)	2
	СР8 Симетричні шифри vs асиметричні шифри	12
Разом	ЛК	16
	ПР	16
	СР	88

Індивідуальне навчально-дослідне завдання:

Детальний розгляд студентами окремих теоретичних положень навчальної дисципліни і формування вміння та навичок їх практичного застосування шляхом виконання поставлених задач.

Методи навчання:

- 1) словесні: лекції, пояснення, розповідь тощо;
- 2) наочні: метод ілюстрацій, метод демонстрацій;
- 3) практичні: практичні заняття;
- 4) робота з літературою: навчально-методична, робота з підручниками і посібниками.

Система оцінювання та вимоги:**Поточна успішність**

- 1** Поточна успішність здобувачів за виконання навчальних видів робіт на навчальних заняттях і за виконання завдань самостійної роботи оцінюється за допомогою чотирибальної шкали оцінок з наступним перерахуванням у 100-бальну шкалу. Під час оцінювання поточної успішності враховуються всі види робіт, передбачені навчальною програмою.
 - 1.1** Лекційні заняття оцінюються шляхом визначення якості виконання конкретизованих завдань.
 - 1.2** Практичні заняття оцінюються якістю виконання контрольного або індивідуального завдання, виконання та оформлення практичної роботи.
- 2** Оцінювання поточної успішності здобувачів вищої освіти здійснюється на кожному практичному занятті (лабораторному чи семінарському) за чотирибальною шкалою («5», «4», «3», «2», «1») і заносяться у журнал обліку академічної успішності.
 - «відмінно» («5»): здобувач бездоганно засвоїв теоретичний матеріал, демонструє глибокі знання з відповідної теми або навчальної дисципліни, основні положення;
 - «добре» («4»): здобувач добре засвоїв теоретичний матеріал, володіє основними аспектами з першоджерел та рекомендованої літератури, аргументовано викладає його; має практичні навички, висловлює свої міркування з приводу тих чи інших проблем, але припускається певних неточностей і похибок у логіці викладу теоретичного змісту або при аналізі практичного;
 - «задовільно» («3»): здобувач в основному опанував теоретичні знання навчальної теми, або дисципліни, орієнтується у першоджерелах та рекомендованій літературі, але непереконливо відповідає, плутає поняття, невпевнено відповідає на додаткові питання, не має стабільних знань; відповідаючи на питання практичного характеру, виявляє неточність у знаннях, не вміє оцінювати факти та явища, пов'язувати їх із майбутньою професією;
 - «незадовільно» («2», «1»): здобувач не опанував навчальний матеріал теми (дисципліни), не знає наукових фактів, визначень, майже не орієнтується в першоджерелах та рекомендованій літературі, відсутнє наукове мислення, практичні навички не сформовані.
- 3** Підсумковий бал за поточну діяльність визнається як середньоарифметична сума балів за кожне заняття, за індивідуальну роботу, поточні контрольні роботи за формулою:

$$K^{поточ} = \frac{K1 + K2 + \dots + Kn}{n},$$

де $K^{поточ}$ – підсумкова оцінка успішності за результатами поточного контролю;

$K_1, K_2, \dots, K_n$ – оцінка успішності n -го заходу поточного контролю;
 n – кількість заходів поточного контролю.
 Оцінки конвертуються у бали згідно шкали перерахунку (таблиця 1).

Підсумкове оцінювання

1 Здобувач вищої освіти отримує залік на останньому занятті з дисципліни за результатами поточного оцінювання. Середня оцінка за поточну діяльність конвертується у бали за 100-бальною шкалою, відповідно до таблиці перерахунку (таблиця 1).

Таблиця 1– Перерахунок середньої оцінки за поточну діяльність у багатобальну шкалу

4-бальна шкала	100-бальна шкала	4-бальна шкала	100-бальна шкала	4-бальна шкала	100-бальна шкала	4-бальна шкала	100-бальна шкала
5	100	4,45	89	3,90	78	3,35	67
4,95	99	4,4	88	3,85	77	3,3	66
4,9	98	4,35	87	3,80	76	3,25	65
4,85	97	4,3	86	3,75	75	3,2	64
4,8	96	4,25	85	3,7	74	3,15	63
4,75	95	4,20	84	3,65	73	3,1	62
4,7	94	4,15	83	3,60	72	3,05	61
4,65	93	4,10	82	3,55	71	3	60
4,6	92	4,05	81	3,5	70	від 1,78 до 2,99 повторне складання	
4,55	91	4,00	80	3,45	69	від 0 до 1,77	від 0 до 34
4,5	90	3,95	79	3,4	68	повторне вивчення	

Здобувачі вищої освіти, які мають середню поточну оцінку з дисципліни нижче ніж «3» (60 балів), на останньому занятті можуть підвищити свій поточний бал шляхом складання тестів з дисципліни.

Оцінювання знань здобувачів шляхом тестування здійснюється за шкалою:

- «відмінно»: не менше 90 % правильних відповідей;
- «дуже добре»: від 82 % до 89 % правильних відповідей;
- «добре»: від 74 % до 81 % правильних відповідей;
- «задовільно»: від 67 % до 73% правильних відповідей;
- «задовільно достатньо»: від 60 % до 66 % правильних відповідей;
- «незадовільно»: менше 60 % правильних відповідей.

2 Умовою отримання заліку є:

- відпрацювання всіх пропущених занять;
- середня поточна оцінка з дисципліни не нижче «3» (60 балів).

3 За виконання індивідуальної самостійної роботи та участь у наукових заходах здобувачам нараховуються додаткові бали.

3.1 Додаткові бали додаються до суми балів, набраних здобувачем вищої освіти за поточну навчальну діяльність.

3.2 Кількість додаткових балів, яка нараховується за різні види індивідуальних завдань, залежить від їх об'єму та значимості:

- призові місця з дисципліни на міжнародному / всеукраїнському конкурсі наукових студентських робіт – 20 балів;
- призові місця з дисципліни на всеукраїнських олімпіадах – 20 балів;
- участь у міжнародному / всеукраїнському конкурсі наукових студентських робіт – 15 балів

- участь у міжнародних / всеукраїнських наукових конференціях студентів та молодих вчених – 12 балів;
- участь у всеукраїнських олімпіадах з дисципліни – 10 балів
- участь в олімпіадах і наукових конференціях ХНАДУ з дисципліни – 5 балів;
- виконання індивідуальних науково-дослідних (навчально-дослідних) завдань підвищеної складності – 5 балів.

3.3 Кількість додаткових балів не може перевищувати 20 балів.

4 Результат навчання оцінюється за двобальною шкалою (зараховано/не зараховано) згідно з таблицею 2. Підсумкова оцінка разом з додатковими балами не може перевищувати 100 балів.

Таблиця 2– Шкала переведення балів у національну систему оцінювання

За 100-бальною шкалою	За національною шкалою
від 60 балів до 100 балів	зараховано
менше 60 балів	незараховано

Визнання результатів неформальної та інформальної освіти

Визнання результатів неформального та (або) інформального навчання здобувача передбачає виконання таких процедур, як: подання здобувачем заяви щодо визнання (не пізніше як протягом перших 10 робочих днів від початку семестру вивчення дисципліни); ідентифікацію задекларованих здобувачем у письмовій формі результатів неформального та (або) інформального навчання; оцінювання задекларованих результатів навчання здобувача; прийняття рішення про визнання та зарахування здобувачу всіх чи частини результатів навчання за дисципліною або відмову у визнанні. Порядок реалізації цих процедур регламентується СТВНЗ 83.1-02:2022 «Визнання результатів навчання, здобутих шляхом неформальної та інформальної освіти»

Політика курсу:

- курс передбачає роботу в колективі, середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики;
 - освоєння дисципліни передбачає обов'язкове відвідування лекцій і практичних занять, а також самостійну роботу;
 - самостійна робота передбачає вивчення окремих тем навчальної дисципліни, які винесені на самостійне опрацювання, або ж були розглянуті стисло;
 - усі завдання, мають бути виконані у встановлений термін;
 - якщо здобувач вищої освіти відсутній на заняттях з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача;
 - курсова робота повинна бути захищена не пізніше, ніж за тиждень до початку екзаменаційної сесії;
 - під час вивчення курсу здобувачі вищої освіти повинні дотримуватись правил академічної доброчесності, викладених у таких документах: «Правила академічної доброчесності учасників освітнього процесу ХНАДУ» (https://www.khadi.kharkov.ua/fileadminZP_Bianbani/poiudeniya/ziynr 67 01 boьrocИ 1.p 67), «Академічна доброчесність. Перевірка тексту академічних, наукових та кваліфікаційних робіт на плагіат» (https://www.khadi.kharkov.ua/fileadminZP_Standart/pologeniya/stvnz 85 1 01.pdf), «Морально-етичний кодекс учасників освітнього процесу ХНАДУ» (https://www.khadi.kharkov.ua/fileadminZP_StandartZpologeniyaZstvnz 67 01 MEK 1.pdf).
 - у разі виявлення факту плагіату здобувач отримує за завдання 0 балів і повинен повторно виконати завдання, які передбачені у силабусі;
- списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних пристроїв). Мобільні пристрої дозволяється використовувати

лише під час он-лайн тестування

Рекомендовані джерела інформації

Основна

1. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
2. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
3. Горбенко В. І., Лісняк А. О. Безпека програм та даних : навчальний посібник для здобувачів ступеня вищої освіти бакалавра спеціальності 121 «Інженерія програмного забезпечення» освітньо-професійної програми «Програмна інженерія». Запоріжжя : ЗНУ, 2022. 72 с.
4. Криптоаналіз. Криптографічні протоколи. Посібник з курсу «Комп'ютерна криптографія» призначено для студентів інженерно-технічного факультету ДВНЗ «УжНУ» спеціальності 123-«комп'ютерна інженерія» / уклад.: О. М. Гапак, 2021.
5. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах : навч. посіб. — Кропивницький: Видавець Лисенко В. Ф., 2020. — 295 с.
6. Класичні методи криптології: методичні рекомендації для здобувачів спеціальностей «Прикладна математика» та «Системний аналіз» / М.М. Повідайчик, І.Я. Шпонтан. Ужгород: Видавництво УжНУ «Говерла», 2020. 28 с.

Допоміжна

1. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Львів: «Новий Світ-2000», 2020 . – 678 с.
2. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології» / В.П. Полторак; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 1,73 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 78 с.
3. Дорогий Я.Ю. Методи та засоби технічного захисту інформації. Практикум: електрон. навч. посіб. / Я.Ю. Дорогий, А.О. Нікітенко – Луцьк: ДонНТУ, 2024. – 241 с.
4. Безпека інформації : конспект лекцій / укладач О. С. Кушнерьов. – Суми : Сумський державний університет, 2021. – 99 с.

Інформаційні ресурси

1. Портал безпека [Електронний ресурс]. – Режим доступу: <https://www.bezpeka.com/uk/golovna/>
2. Верховна Рада України. Законодавство України: [Електронний ресурс]. – Режим доступу: <http://zakon.rada.gov.ua/laws/>
3. Державна служба спеціального зв'язку та захисту інформації: [Електронний ресурс]. – Режим доступу: <https://cip.gov.ua/ua>
4. Команда реагування на комп'ютерні надзвичайні події України: [Електронний ресурс]. – Режим доступу: <https://cert.gov.ua/>

Розробник силабусу навчальної дисципліни

к.т.н., доцент



Михайло ПІКСАСОВ

Завідувач кафедри кібербезпеки

к.т.н., доцент



Олена КРАЙНЮК