

Силабус Освітнього компоненту ВД

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=2897
Обсяг освітнього компоненту	4 кредита (120 годин)
Форма підсумкового контролю	Залік
Консультації:	за графіком
Назва кафедри:	кафедра комп'ютерних систем
Мова викладання:	українська
Керівник курсу:	Неронов сергій миколайович, старший викладач кафедри КС
Контактний телефон:	+38-067-703-64-16
E-mail:	sernikner@gmail.com

Пререквизити та постреквизити навчальної дисципліни:

- **Пререквизити:** «Алгоритмізація та програмування», «Об'єктно-орієнтоване програмування», «Бази даних», «Комп'ютерна графіка».
- **Постреквизити:** «Тестування програмного забезпечення», «Програмування баз даних».

Характеристика дисципліни:

Призначення навчальної дисципліни: Навчальна дисципліна «Технології захисту інформації» є загально дисципліною і входить в професійний цикл, який формує базовий рівень знань для освоєння загально-професійних навичок.

Мета вивчення навчальної дисципліни надати основні відомості з принципів побудови систем захисту інформації та методів протидії спробам несанкціонованого доступу до неї з боку сторонніх осіб, привласнення привілеїв тощо.

Задачі вивчення дисципліни: По завершенні вивчення дисципліни студенти повинні:

знати:

- об'єкти програмного забезпечення, на які можливі атаки з боку комп'ютерних хакерів, та методи здійснення несанкціонованого доступу до інформації;
- принципи функціонування вбудованих засобів захисту комп'ютерних систем
- (BIOS) та шляхи протидії спробам їх взлому;
- принципи функціонування систем захисту, призначення привілеїв, зберігання паролів та автентифікація користувачів в операційних системах WINDOWS, та UNIX, методи хакерів з несанкціонованого проникнення до інформації, привласнення привілеїв адміністратора тощо;

– методи несанкціонованого зйому та навмисного пошкодження інформації

вмісту:

– використовувати засоби протидії цим спробам;
– використовувати методи побудови захисту окремих програмних продуктів;

– використовувати основні прийоми і програмні засоби для аналізу та дизасемблювання програмних продуктів з метою їх подальшого несанкціонованого використання,

– використовувати методи захисту від дизасемблювання.

Зміст навчальної дисципліни: відповідає навчальній та робочій програмі, яка відповідає запитам роботодавців

№ теми	Назва тем (ЛК, ЛР, ПР, СЗ, СР)	Кількість годин
		очна
1	ЛК Складові «Інформаційної безпеки», Основні поняття та задачі криптології	2
	ПР (ЛР, СЗ) Класичний шифр простої заміни та його криптоаналіз. біграмний шифр	2
	СР Види шифрів	11
2	ЛК . Безпека в інформаційних мережах. Фізична безпека. Загальна характеристика систем захисту в інформаційних мережах	2
	ПР (ЛР, СЗ) . Автентифікація та безпека мережі. Паролі. Користувацький інтерфейс.	2
	СР Телекомунікації та віддалений доступ. Резервне копіювання. Адміністрування інформаційних систем	11
3	ЛК Класичні шифри та їх криптоаналіз	2
	ПР (ЛР, СЗ) Класичний шифр поліалфавітної заміни та його криптоаналіз. криптосистема хілла	2
	СР Моноалфавітний шифр	11
4	ЛК Криптографічна стійкість шифрів	2
	ПР (ЛР, СЗ) Моделювання процесів шифрування за допомогою операції XOR. Алгоритм DES	2
	СР Типи атак на криптосистеми	11
5	ЛК Система захисту комп'ютера з допомогою BIOS	2
	ПР (ЛР, СЗ) Налаштування особистого захисту ПК.	2
	СР Види BIOS	11
6	ЛК Удосконалений стандарт шифрування AES	2
	ПР (ЛР, СЗ) Алгоритм AES	2
	СР Режими виконання блокових шифрів	9
7	ЛК Національний стандарт шифрування ДСТУ 7624:2014 («Калина»)	2
	ПР (ЛР, СЗ) Режими роботи «Калина»	2
	СР «Калина» vs AES	11
8	ЛК Основні положення криптографії з відкритим ключем	2
	ПР (ЛР, СЗ) Алгоритм рюкзака (криптосистема Меркла-Хелмана)	2
	СР Симетричні шифри vs асиметричні шифри	11
Разом	ЛК	16
	ПР (ЛР, СЗ)	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: 1.1 традиційні: лекції, пояснення, розповідь тощо;
- 1.2 інтерактивні (нетрадиційні): проблемні лекції, дискусії тощо;
- 2) наочні: метод ілюстрацій, метод демонстрацій
- 3) практичні: 3.1 традиційні: практичні заняття, семінари;
- 3.2 інтерактивні (нетрадиційні): тренінги, «круглий стіл», метод мозкової атаки.

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.

1.3 Лабораторні заняття оцінюються якістю виконання звітів про виконання лабораторних робіт.

1.4 Семінарські заняття оцінюються якістю виконання індивідуального завдання/реферату.

2 Оцінювання поточної успішності здобувачів вищої освіти здійснюється на кожному практичному занятті (лабораторному чи семінарському) за чотирибальною шкалою («5», «4», «3», «2») і заносяться у журнал обліку академічної успішності.

– «відмінно»: здобувач бездоганно засвоїв теоретичний матеріал, демонструє глибокі знання з відповідної теми або навчальної дисципліни, основні положення;

– «добре»: 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»: 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»: 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;

$K1, K2, \dots, Kn$ – оцінка успішності n -го заходу поточного контролю;

n – кількість заходів поточного контролю.

Оцінки конвертуються у бали згідно шкали 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	

Підсумкове оцінювання

1 Екзамен проводиться після вивчення всіх тем дисципліни і складається здобувачами вищої освіти в період екзаменаційної сесії після закінчення всіх аудиторних занять

2 До екзамену допускаються здобувачі вищої освіти, які виконали всі види робіт передбачені навчальним планом з дисципліни:

- були присутні на всіх аудиторних заняттях (лекції, семінари, практичні);
- своєчасно відпрацювали всі пропущені заняття;
- набрали мінімальну кількість балів за поточну успішність (не менше 36 балів, що відповідає за національною шкалою «3»);

Якщо поточна успішність з дисципліни нижче ніж 36 балів, здобувач вищої освіти має можливість підвищити свій поточний бал до мінімального до початку екзаменаційної сесії.

3 Оцінювання знань здобувачів при складанні екзамену здійснюється за 100-бальною шкалою.

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.

4 Підсумкова оцінка з навчальної дисципліни визначається як середньозважена оцінка, що враховує загальну оцінку за поточну успішність і оцінку за складання екзамену.

5 Розрахунок загальної підсумкової оцінки за вивчення навчальної дисципліни проводиться за формулою:

$$PK^{екз} = 0,6 \cdot K^{поточ} + 0,4 \cdot E ,$$

де $PK^{екз}$ – підсумкова оцінка успішності з дисциплін, формою підсумкового контролю для яких є екзамен;

$K^{поточ}$ – підсумкова оцінка успішності за результатами поточного контролю (за 100-бальною шкалою);

E - оцінка за результатами складання екзамену (за 100-бальною шкалою).

0,6 і 0,4 – коефіцієнти співвідношення балів за поточну успішність і складання екзамену.

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

6.1 Додаткові бали додаються до суми балів, набраних здобувачем вищої освіти за поточну навчальну діяльність (для дисциплін, підсумковою формою контролю для яких є залік), або до підсумкової оцінки з дисципліни, підсумковою формою контролю для якої є екзамен.

6.2 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.

6.3 Кількість додаткових балів не може перевищувати 20 балів.

7 Загальна підсумкова оцінка за вивчення навчальної дисципліни не може перевищувати 100 балів.

Загальна підсумкова оцінка за вивчення навчальної дисципліни визначається згідно зі шкалою, наведеною в таблиці 2.

Таблиця 2 – Шкала оцінювання знань здобувачів за результатами підсумкового контролю з навчальної дисципліни

Оцінка в балах	Оцінка за національною шкалою		Оцінка за шкалою ЄКТС	
	екзамен	залік	Оцінка	Критерії
90-100	Відмінно	Зараховано	A	Теоретичний зміст курсу освоєний цілком, без прогалин, необхідні практичні навички роботи з освоєним матеріалом сформовані, усі передбачені програмою навчання навчальні завдання виконані, якість їхнього виконання оцінено числом балів, близьким до максимального
80–89			B	Теоретичний зміст курсу освоєний цілком, без прогалин, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, усі передбачені програмою навчання навчальні завдання виконані, якість виконання більшості з них оцінено числом балів, близьким до максимального
75-79			C	Теоретичний зміст курсу освоєний цілком, без прогалин, деякі практичні навички роботи з освоєним матеріалом сформовані недостатньо, усі передбачені програмою навчання навчальні завдання виконані, якість виконання жодного з них не оцінено мінімальним числом балів, деякі види завдань виконані з помилками
67-74			D	Теоретичний зміст курсу освоєний частково, але прогалини не носять істотного характеру, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконано, деякі з виконаних завдань, можливо, містять помилки
60–66			E	Теоретичний зміст курсу освоєний частково, деякі практичні навички роботи не сформовані, багато передбачених програмою навчання навчальних завдань не виконані, або якість виконання деяких з них оцінено числом балів, близьким до мінімального.

Оцінка в балах	Оцінка за національною шкалою		Оцінка за шкалою ЄКТС	
			Оцінка	Критерії
	екзамен	залік		
35–59	Незадовільно	Не зараховано	FX	Теоретичний зміст курсу освоєний частково, необхідні практичні навички роботи не сформовані, більшість передбачених програм навчання навчальних завдань не виконано, або якість їхнього виконання оцінено числом балів, близьким до мінімального; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання)
0–34			F	Теоретичний зміст курсу не освоєно, необхідні практичні навички роботи не сформовані, усі виконані навчальні завдання містять грубі помилки, додаткова самостійна робота над матеріалом курсу не приведе до якого-небудь значущого підвищення якості виконання навчальних завдань (з обов'язковим повторним курсом)

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 відповідно до програми на самостійне опрацювання, або ж були розглянуті стисло;
- усі завдання, передбачені програмою, 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/fileadmin/P_Standart/pologeniya/stvnz_67_01_dobroch_1.pdf), «Академічна доброчесність. Перевірка тексту академічних, наукових та кваліфікаційних робіт на плагіат» (https://www.khadi.kharkov.ua/fileadmin/P_Standart/pologeniya/stvnz_85_1_01.pdf), «Морально-етичний кодекс учасників освітнього процесу ХНАДУ» (https://www.khadi.kharkov.ua/fileadmin/P_Standart/pologeniya/stvnz_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. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Чинний з 29.12.2014 р. ПАТ «Інститут інформаційних технологій» Мінекономрозвитку України, 2016.– 228 с.
2. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція хешування. – Чинний з 29.12.2014 р. – ПАТ «Інститут інформаційних технологій» Мінекономрозвитку України, 2016. – 228 с.
3. Ляшенко І.О. Європейські критерії безпеки інформаційних технологій / І.О. Ляшенко // Сучасні інформаційні технології у сфері безпеки та оборони. – 2014. – № 1 (13). – С. 84–86.
4. Про електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. Відомості Верховної Ради України. 2017, № 45, ст. 400. URL: <https://zakon.rada.gov.ua/laws/show/2155-19>.
5. Тарнавський Ю. А. Технології захисту інформації: підручник / Ю.А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
6. Токен – новий вид інформації. Газета «Інтерактивна бухгалтерія» №128 /2019. URL: <https://interbuh.com.ua/ua/documents/oneanalytics/131413>
7. Хорошко В.О. Основи інформаційної безпеки: підручник / В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест; за ред.В.О. Хорошка. – К.: ДУІКТ, 2017. – 186 с.

Допоміжна

8. Ковальчук Л.В. О криптографических свойствах нового национального стандарта шифрования украины /Ковальчук Л.В. //Кибернетика и системный анализ. — 2016. — Т. 52, № 3. — С. 16-32.
9. Яковлев С.В. Уточнені оцінки стійкості алгоритму шифрування ДСТУ 7624:2014 до диференціального та лінійного криптоаналізу /Яковлев С.В. /Інформаційні технології та комп'ютерна інженерія. — 2015. — С. 176-178.
10. Яковлев С.В. Аналітичні оцінки стійкості немарковських симетричних блочних шифрів до диференціального криптоаналізу : кандидатська дисертація / Яковлев С.В. — К.: НТУУ «КШ», 2016. — 160 с.

Інтернет-джерела

– <http://www.google.com/>

– Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України: нормативно-правова база. – Режим доступу: www.dstszi.gov.ua/dstszi/control/uk/index

Розробник (розробники)

силабусу навчальної дисципліни _____

Сергій НЕРОНОВ

підпис

ПІБ

Завідувач кафедри

підпис

Віталіна БАБЕНКО

ПІБ

