СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Інформаційна безпека комп'ютерних систем»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Василенко Володимир Вікторович, кандидат технічних наук, доцент.</td><td colspan="2">Контактна інформація лектора (e-mail), сторінка курсу в Moodle</td><td colspan="2">e-mail: oknelisavvova172@gmail.com; сторінка курсу в Moodle – http://dl.dut.edu.ua/course/view.php?id=171076</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2">12 «Інформаційні технології»</td><td colspan="2">Рівень вищої освіти</td><td colspan="2">бакалавр</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2">122 Комп’ютерні науки</td><td colspan="2">Семестр</td><td colspan="2">5</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2">Штучний інтелект</td><td colspan="2">Тип дисципліни</td><td colspan="2">Обов’язкова</td></tr>
<tr><td rowspan="2">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="6">За видами занять:</td></tr>
<tr><td>3</td><td>90</td><td>Лекцій
18</td><td>Семінарських занять
-</td><td>Практичних занять
18</td><td>Лабораторних занять
18</td><td colspan="2">Самостійна підготовка
36</td></tr>
<tr><td colspan="9">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="9">Взаємозв’язок у структурно-логічній схемі</td></tr>
<tr><td colspan="3">Освітні компоненти, які передують вивченню</td><td colspan="6">1. Алгоритмізація та програмування
2. Бази даних
3. Конвергентна ме режна інфраструктура
4. Прикладне програмування–JAVA
5. Серверні операційні системи</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="6">1. Штучний інтелект
2. Виробнича практика
3. Хмарна платформа OpenSteck
4. Серверні платформи HPE</td></tr>
<tr><td>Мета курсу:</td><td colspan="8">Мета курсу "Інформаційна безпека комп'ютерних систем" полягає в забезпеченні студентів необхідними знаннями, навичками та уміннями для розуміння, виявлення та ефективного управління ризиками, пов'язаними з інформаційною безпекою в сучасних комп'ютерних системах. Курс спрямований на формування у студентів розуміння загроз, які можуть виникнути у віртуальному просторі, та розробку стратегій та заходів для їх запобігання та подолання.</td></tr>
<tr><td colspan="9">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="5">Soft- skills / Загальні компетентності (ЗК)</td><td colspan="4">Hard-skills / Спеціальні компетентності (СК)</td></tr>
<tr><td colspan="5">ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК2. Здатність застосовувати знання у практичних ситуаціях.
ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК5. Здатність спілкуватися іноземною мовою.
ЗК6. Здатність вчитися й оволодівати сучасними знаннями.
ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК11. Здатність приймати обґрунтовані рішення.
ЗК13. Здатність діяти на основі етичних міркувань.
ЗК14. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства</td><td colspan="4">СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури.</td></tr>
</table>

та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. **ЗК15.** Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.	

Програмні результати навчання (ПР)

ПР1. Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук.
ПР15. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Тема 1. Вступ до інформаційної безпеки ***Знати***: класифікацію, види та функції напрямів інформаційної безпеки. ***Вміти:*** орієнтуватися у переліку термінів ІБ які використовуються в наявних проектах. ***Формування компетенцій:*** ЗК1, ЗК2, ЗК4, ЗК5, ЗК6, ЗК7, ЗК11, ЗК13, ЗК14, ЗК15, СК14 ***Програмні результати навчання:*** ПР1, ПР15 ***Рекомендовані джерела:*** 1-4			
Заняття 1.1 Вступ до інформаційної безпеки	Лекція 1 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 1.2 Виклики та проблеми інформаційної безпеки	Лекція 2 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 1.3. Основи роботи з операційною системою з точки зору безпеки	Практичне заняття 1 4 год	5 балів	Усне опитування, навчальна дискусія, ситуаційне завдання
Заняття 1.4. Питання для розуміння базових принципів інформаційної безпеки та основ операційних систем	Лабораторне заняття 1 4 год	5 балів	Тестування

Тема 2. Криптографія ***Знати***: Терміни і поняття криптографії. Типи шифрування. Типи кодування. ***Вміти***: Зробити шифрування та дешифрування інформації. ***Формування компетенцій:*** ЗК1, ЗК2, ЗК4, ЗК5, ЗК6, ЗК7, ЗК11, ЗК13, ЗК14, ЗК15, СК14 ***Програмні результати навчання:*** ПР1, ПР15 ***Рекомендовані джерела:*** 1–4			
Заняття 2.1 Вступ до криптографії.	Лекція 3 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 2.1 Шифрування, Кодування, Хешування	Лекція 4 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 2.2. Робота з криптографічними алгоритмами та шифруванням	Практичне заняття 2 4 год	5 балів	Усне опитування, навчальна дискусія, ситуаційне завдання
Заняття 2.3. Питання для перевірки розуміння та застосування криптографічних алгоритмів	Лабораторне заняття 2 4 год	5 балів	Тестування
Тема 3. Управління доступом та ідентифікація ***Знати***: Терміни і поняття управління доступом та ідентифікація. Матриці доступів. ***Вміти***: Налаштувати доступ до системи. ***Формування компетенцій:*** ЗК1, ЗК2, ЗК4, ЗК5, ЗК6, ЗК7, ЗК11, ЗК13, ЗК14, ЗК15, СК14 ***Програмні результати навчання:*** ПР1, ПР15 ***Рекомендовані джерела:*** 1–5			
Заняття 3.1 Управління доступом та ідентифікація	Лекція 5 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 3.2. Створення та налаштування політик доступу	Практичне заняття 3 2 год	3 бали	Усне опитування, навчальна дискусія, ситуаційне завдання
Заняття 3.3. Питання для перевірки розуміння систем ідентифікації та управління доступом	Лабораторне заняття 3 2 год	3 бали	Тестування

Тема 4. Мережева безпека ***Знати***: Терміни і поняття мережевої безпеки. Розуміння сенсу роботи мережевих фаєрволів. ***Вміти***: Налаштувати мережевий фаервол. ***Формування компетенцій:*** ЗК1, ЗК2, ЗК4, ЗК5, ЗК6, ЗК7, ЗК11, ЗК13, ЗК14, ЗК15, СК14 ***Програмні результати навчання:*** ПР1, ПР15 ***Рекомендовані джерела:*** 1–6			
Заняття 4.1 Мережева безпека.	Лекція 6 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 4.2. Робота з мережевими брандмауерами та системами виявлення вторгнень	Практичне заняття 4 2 год	2 бали	Усне опитування, навчальна дискусія, ситуаційне завдання
Заняття 4.3. Питання для перевірки розуміння принципів роботи мережевих захисних механізм	Лабораторне заняття 4 2 год	3 бали	Тестування
Тема 5. Безпека веб-застосунків. ***Знати***: Терміни і поняття безпеки веб-застасунків. Вразливості в веб-застосунках. ***Вміти***: Відрізняти різні типи вразливостей, та застосувати відповідні типи захистів. ***Формування компетенцій:*** ЗК1, ЗК2, ЗК4, ЗК5, ЗК6, ЗК7, ЗК11, ЗК13, ЗК14, ЗК15, СК14 ***Програмні результати навчання:*** ПР1, ПР15 ***Рекомендовані джерела:*** 1–7			
Заняття 5.1 Безпека веб-застосунків.	Лекція 7 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 5.2. Аудит безпеки веб-застосунків	Практичне заняття 5 2 год	2 бали	Усне опитування, навчальна дискусія, ситуаційне завдання
Заняття 5.3. Тестове завдання Безпека веб-застосунків	Лабораторне заняття 5 2 год	3 бали	Тестування

Тема 6. Безпека мобільних пристроїв ***Знати***: Терміни і поняття безпеки мобільних пристроїв. ***Вміти***: Налаштувати безпеку мобільних простроїв. ***Формування компетенцій:*** ЗК1, ЗК2, ЗК4, ЗК5, ЗК6, ЗК7, ЗК11, ЗК13, ЗК14, ЗК15, СК14 ***Програмні результати навчання:*** ПР1, ПР15 ***Рекомендовані джерела:*** 1–8			
Заняття 6.1 Безпека мобільних пристроїв	Лекція 8 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 6.2 Використання безкоштовного Android Studio для вивчення безпеки мобільних застосунків	Практичне заняття 6 2 год	2 бали	Усне опитування, навчальна дискусія, ситуаційне завдання.
Заняття 6.3 Питання для перевірки розуміння принципів роботи безпеки мобільних застосунків	Лабораторне заняття 6 2 год	3 бали	Тестування
Тема 7. Хмарна інформаційна безпека ***Знати***: Терміни і поняття хмарної безпеки. ***Вміти***: Налаштувати сервіси безпеки у хмарному середовищі. ***Формування компетенцій:*** ЗК1, ЗК2, ЗК4, ЗК5, ЗК6, ЗК7, ЗК11, ЗК13, ЗК14, ЗК15, СК14 ***Програмні результати навчання:*** ПР1, ПР15 ***Рекомендовані джерела:*** 1–10			
Заняття 7.1 Хмарна інформаційна безпека.	Лекція 9 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 7.2. Робота з налаштуваннями безпеки хмарних провайдерів	Практичне заняття 7 2 год	2 бали	Усне опитування, навчальна дискусія, ситуаційне завдання
Заняття 7.3. Питання для перевірки розуміння та налаштування безпеки хмарних провайдерів	Лабораторне заняття 7 2 год	3 бали	Тестування

Тема 1. Вступ до інформаційної безпеки	Самостійна робота 1. 5 годин	2 бали	1. Основні принципи інформаційної безпеки. 2. Технології та методи захисту інформації. 3. Соціальна інженерія та атаки на людину. Управління інформаційною безпекою в організаціях.
Тема 2. Криптографія	Самостійна робота 2. 5 годин	2 бали	1. Основні принципи криптографії. 2. Типи криптографічних алгоритмів та їх застосування. 3. Шифрування та дешифрування повідомлень. Застосування криптографії в інформаційній безпеці.
Тема 3. Управління доступом та ідентифікація	Самостійна робота 3. 5 годин	2 бали	1. Огляд методів ідентифікації в інформаційних системах. 2. Технології біометричної ідентифікації та їх застосування. 3. Моделі та стратегії управління доступом. Аудит та моніторинг систем управління доступом.
Тема 4. Мережева безпека	Самостійна робота 4. 5 годин	2 бали	1. Аналіз загроз та вразливостей в мережевій безпеці. 2. Технології шифрування та захисту даних в мережах. 3. Методи виявлення та запобігання атакам в мережах. Управління та моніторинг мережевою безпекою.
Тема 5. Безпека веб-застосунків	Самостійна робота 5. 5 годин	2 бали	1. Уразливості веб-застосунків та їх вплив на безпеку. 2. Методи аутентифікації та авторизації в веб-застосунках. 3. Захист від кросс-сайт атак та інших загроз безпеці веб-додатків. Моніторинг та аудит безпеки веб-застосунків.
Тема 6. Безпека мобільних пристроїв	Самостійна робота 6. 5 годин	2 бали	1. Уразливості та загрози для безпеки мобільних пристроїв. 2. Методи шифрування та захисту даних на мобільних пристроях. 3. Захист від мобільних вірусів та шкідливих додатків. Стратегії управління доступом та конфіденційність на мобільних платформах.
Тема 7. Хмарна інформаційна безпека	Самостійна робота 7. 6 годин	2 бали	1. Хмарні платформи та їхні основні принципи безпеки. 2. Методи шифрування та захисту даних в хмарних сервісах. 3. Управління ідентифікацією та доступом в хмарних оточеннях. Моніторинг та аудит безпеки в хмарних інфраструктурах
МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			
● Мультимедійний проектор; ● Комп’ютерний клас для проведення практичних занять.			
ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			

1. William Stallings. "Cryptography and Network Security: Principles and Practice." Pearson, 2016. (784 p.) - https://www.pearson.com/us/higher-education/program/Stallings-Cryptography-and-Network-Security-Principles-and-Practice-7th-Edition/PGM335896.html
2. Ross Anderson. "Security Engineering: A Guide to Building Dependable Distributed Systems." Wiley, 2020. (1024 p.) - https://www.wiley.com/en-us/Security+Engineering%3A+A+Guide+to+Building+Dependable+Distributed+Systems%2C+3rd+Edition-p-9781119642787
3. ISO/IEC 27001:2013. "Information technology — Security techniques — Information security management systems — Requirements." - https://www.iso.org/standard/54534.html
4. NIST Special Publication 800-53. "Security and Privacy Controls for Federal Information Systems and Organizations." - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
5. Bruce Schneier. "Secrets and Lies: Digital Security in a Networked World." Wiley, 2004. (448 p.) - https://www.schneier.com/books/secrets-and-lies/
6. Kevin D. Mitnick. "The Art of Deception: Controlling the Human Element of Security." Wiley, 2002. (368 p.) - https://www.wiley.com/en-us/The+Art+of+Deception%3A+Controlling+the+Human+Element+of+Security-p-9780764542800
7. "National Cyber Security Centre (NCSC)" - Various publications and recommendations. - https://www.ncsc.gov.uk/
8. Brian Krebs. "Krebs on Security" - Online blog focusing on cybersecurity. - https://krebsonsecurity.com/
9. Virtual Hacking Labs - Practical labs for ethical hacking and penetration testing. - https://www.virtualhackinglabs.com/
10. Coursera: "Cybersecurity Specialization" - Various courses from leading universities. - https://www.coursera.org/specializations/intro-cyber-security

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- 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 включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблене опрацювання за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації студент повинен вказати джерело, використане в ході виконання завдання. Виявлення ознак академічної недоброчесності в практичній (письмовій) роботі студента є підставою для її незарахування викладачем.
- Студент, який спізнився має право бути присутнім на занятті. Студенти мають інформувати старосту про неможливість відвідати заняття.
- Користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням є підставою для незарахування викладачем роботи студента.

КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є виконання всіх практичних робіт і виконання самостійних завдань, які передбачені структурою освітньої компоненти Інформаційна безпека комп'ютерних систем.

Якщо студента не допущено до складання заліку, як такого, що не виконав індивідуальний план, йому надається час до перескладання для виконання всіх вимог допуску. Студент має право на два перескладання. При повторному перескладанні екзамену його у студента може приймати комісія, яка створюється директором ННІІТ. Оцінка комісії є остаточною. У випадку отримання студентом 0 балів (неприйнятно), що тягне відрахування за невиконання навчального плану.

Оцінювання студентів здійснюється за накопичувальною 100-бальною системою і складається із двох основних оцінкових блоків і розподіляється в певних пропорціях 60 *(бали напрацьовані під час вивчення дисципліни – Поточний контроль)*, 40 *(підсумкове оцінювання - екзамен)*:

Форми контролю	**Види навчальної роботи**	**Оцінювання**

ПОТОЧНИЙ КОНТРОЛЬ	●Виконання тестових завдань робіт	46 балів
	●Самостійна робота	14 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ *екзамен*	Екзамен проходить у тестовій формі.	40 балів

Додаткова оцінка	
Види навчальної роботи	**Оцінювання**
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:	
- Тези доповіді на фаховій конференції	3 бали
- Стаття у фаховому виданні	5 балів
- Стаття в іноземному рецензованому виданні	10 балів
Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти - 10 балів.	

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90-100	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об‘єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов’язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об’єму матеріалу, передбаченого робочою програмою, або студент проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)
82-89	Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних	**Достатній** Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені	Добре / Зараховано (В)

	завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	дисципліни	
75-81	Студент в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)
64-74	Студент засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-63	Студент має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, студент з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі екзамену/заліку.	**Незадовільний** Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*