ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
Силабус навчальної дисципліни

БЕЗПЕКА КІБЕРФІЗИЧНИХ СИСТЕМ

Викладач: *Горелікова Тетяна Олексіївна*
Кафедра: *комп'ютерних наук, І корпус, ауд. 39*
E-mail: *horelikova.t@znu.edu.ua*
Телефон: *(061) 289-12-57*
Інші засоби зв'язку: M*oodle (форум курсу, приватні повідомлення)*

Освітня програма, рівень вищої освіти:		Кібербезпека та захист інформації Бакалавр					
Статус дисципліни:		Обов'язкова					
Кредити ECTS	4	**Навч. рік:**	2026-2027 1 семестр	**Рік навчання**	4	**Тижні**	16
Кількість годин	120	**Кількість змістових модулів**	4	**Лекційні заняття** – 16 год **Лабораторні заняття** – 16 год **Самостійна робота** – 88 год			
Вид контролю:		Іспит					
Посилання на курс в Moodle		https://moodle.znu.edu.ua/course/view.php?id=18586					
Консультації: Запис на консультації: особисті повідомлення в Moodle							

ОПИС КУРСУ

Навчальна дисципліна «Безпека кіберфізичних систем» спрямована на вивчення теоретичних засад і практичних методів забезпечення захищеності систем, у яких цифрові технології безпосередньо керують фізичними процесами та технологічними об'єктами. У межах курсу розглядаються архітектура кіберфізичних систем, моделювання загроз, особливості захисту сенсорів, виконавчих механізмів і промислових мереж. Значну увагу приділено безпеці вбудованих пристроїв, захищеному завантаженню програмного забезпечення, контролю цілісності та застосуванню криптографічних механізмів захисту. Також вивчаються методи сегментації мереж, виявлення вторгнень, журналювання подій і протидії мережевим атакам. У результаті опанування дисципліни здобувач набуває компетентностей щодо проєктування, впровадження та супроводу комплексних рішень із забезпечення безпеки кіберфізичних систем.

Програмні результати навчання	
ПРН1	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень
ПРН2	Забезпечувати процеси захисту та функціонування інформаційно- телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент
ПРН3	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
ПРН4	Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах

ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ

Презентації лекцій, презентаційні та відео матеріали, завдання та методичні рекомендації до практичних занять і самостійної роботи, методичне забезпечення поточного і підсумкового контроля, основна та додаткова література розміщені на платформі Moodle.

РОЗКЛАД КУРСУ ЗА ТЕМАМИ І КОНТРОЛЬНІ ЗАВДАННЯ

Поточні контрольні заходи

Основними контрольними заходами є завдання практичних занять, завдання самостійних робіт й тести, які виконуються після опанування відповідної теми курсу. Всі поточні контрольні заходи та методичні рекомендації до їх виконання розташовані на платформі Moodle.

Підсумкові контрольні заходи

Індивідуальне завдання. *Захищений модуль керування та аналіз безпеки програмного забезпечення для об'єкта кіберфізичних систем (перелік об'єктів та варіантів наведено в завданні). 20 балів. Завдання, вихідні дані та перелік варіантів робіт наведено в завданні на платформі Moodle.*

Підсумковий контроль (іспит). *Виконання практичних завдань екзаменаційного білету – 20 балів (проводиться письмово в аудиторії або онлайн на платформі Moodle).*

Тиждень і вид заняття	**Тема заняття**	**Контрольні заходи, кількість балів**
Змістовий модуль 1. Основи безпеки кіберфізичних систем та оцінка ризиків у фізичному середовищі		
Тиждень 1 Лекція 1	Поняття кіберфізичних систем, їхня архітектура та відмінності від стандартних інформаційних систем.	–
Тиждень 2 Самостійна робота	Дослідження реальних аварій у промислових системах, викликаних програмними помилками.	*Самостійна робота №1.* Аналіз причин та наслідків програмних збоїв у критичній інфраструктурі. (*max 1 бали*)
Тиждень 2 Практичне заняття 1	Аналіз взаємодії програмного забезпечення з фізичним обладнанням на прикладі систем автоматизації.	*Практичне завдання №1.* Відстеження ланцюжка керування: від програмної команди до дії виконавчого механізму. (*max 4 бали*)
Тиждень 2 Самостійна робота	Порівняльний аналіз вимог до безпеки даних та вимог до фізичної безпеки обладнання.	*Самостійна робота №2.* Формулювання вимог до безпеки життєдіяльності та доступності для виконавчих пристроїв. (*max 1 бали*)
Тиждень 3 Лекція 2	Методологія моделювання загроз та виявлення аномальних показників вимірювальних приладів	–
Тиждень 3 Самостійна робота	Класифікація можливих порушень у роботі виконавчих механізмів та приводів.	*Самостійна робота №3.* Систематизація фізичних наслідків від несанкціонованого втручання в керування виконавчою системою та приводами. (*max 1 бали*)
Тиждень 4 Практичне заняття 2	Алгоритмічна перевірка правдоподібності значень датчиків у програмному коді.	*Практичне завдання №2.* Розробка програмного модуля виявлення аномальних та підроблених показників сенсорів. (*max 4 бали*)

Тиждень і вид заняття	**Тема заняття**	**Контрольні заходи, кількість балів**
Тиждень 4	Оцінка стійкості вимірювальних систем до зовнішніх інформаційних впливів	*Тест №1.* (*max 5 бали*)
Змістовий модуль 2. Безпека низькорівневого програмного забезпечення та прошивок		
Тиждень 5 Лекція 3	Низькорівневі вразливості оперативної пам'яті та методи їхнього усунення у програмному коді.	–
Тиждень 6 Практичне заняття 3	Усунення вразливостей пам'яті та реалізація перевірки цифрового підпису програмного забезпечення.	*Практичне завдання №3.* Усунення вразливостей пам’яті та налаштування перевірки цифрового підпису прошивки. (*max 4 бали*)
Тиждень 7 Лекція 4	Методи перевірки виконуваних файлів та механізми безпечної дистанційної заміни прошивок.	–
Тиждень 7 Самостійна робота	Вивчення структур файлів прошивок для різних архітектур процесорів.	*Самостійна робота №4.* Аналіз заголовочних структур та розподілу пам'яті у виконуваних файлах. (*max 1 бали*)
Тиждень 8 Практичне заняття 4	Аналіз бінарних образів та розробка сценарію захищеного оновлення програмного забезпечення.	*Практичне завдання №4.* Аналіз прошивки та налаштування її автоматичного оновлення. (*max 4 бали*)
Тиждень 8	Аудит безпеки вбудованого програмного забезпечення та механізмів його захисту	*Тест №2.* (*max 5 бали*)
Змістовий модуль 3. Захист мережевої взаємодії та спеціалізованих протоколів		
Тиждень 9 Лекція 5	Принципи побудови технологічних мереж та специфіка промислових протоколів.	–
Тиждень 10 Практичне заняття 5	Вивчення методів розділення внутрішніх мереж на ізольовані сегменти	*Практичне завдання №5.* Принципи міжмережевого екранування та сегментації систем. (*max 4 бали*)
Тиждень 10 Самостійна робота	Огляд компактних алгоритмів шифрування для малопотужних пристроїв.	*Самостійна робота №5. П*ротоколи безпеки для обмежених у ресурсах пристроїв. (*max 1 бали*)
Тиждень 11 Лекція 6	Мережеві атаки на внутрішні канали зв'язку та заходи захисту.	–

Тиждень і вид заняття	**Тема заняття**	**Контрольні заходи, кількість балів**
Тиждень 11 Самостійна робота	Перевірка автентичності відправника та виявлення підроблених мережевих адрес.	*Самостійна робота №6.* Методи перевірки автентичності мережевого обладнання. (*max 1 бали*)
Тиждень 12 Практичне заняття 6	Захист від повторного відправлення команд та оцінка навантаження на систему.	*Практичне завдання №6.* Блокування повторних мережевих запитів та вимірювання швидкодії шифрування. (*max 4 бали*)
Тиждень 12 Самостійна робота	Оптимізація обміну ключами для бездротових датчиків.	*Самостійна робота №7.* Протоколи безпечної передачі ключів у сенсорних мережах. (*max 1 бали*)
Тиждень 12	Захист мережевої взаємодії у розподілених системах	*Тест №3.* (*max 5 бали*)
Змістовий модуль 4. Забезпечення якості коду, моніторинг та реагування		
Тиждень 13 Лекція 7	Стандарти надійного кодування та алгоритми виявлення відхилень від нормального режиму роботи.	–
Тиждень 14 Практичне заняття 7	Вивчення принципів журналювання подій у системі без можливості їх підробки.	*Практичне завдання №7.* Проектування захищеної системи реєстрації системних подій із захистом від зміни історії. (*max 4 бали*)
Тиждень 15 Лекція 8	Стратегії збереження працездатності та локалізації збоїв у критичних вузлах.	–
Тиждень 14 Самостійна робота	Опрацювання способів ізоляції системних помилок для запобігання повному зупиненню обладнання.	*Самостійна робота №8.* Методи ізоляції програмних помилок у критичних системах. (*max 1 бали*)
Тиждень 16 Практичне заняття 8	Автоматизоване випробування спотвореними даними та розробка інструкцій з реагування на збої.	*Практичне завдання №8.* Перевірка стійкості мережевого інтерфейсу викривленими даними та розробка регламенту дій при компрометації пристрою. (*max 4 бали*)
Тиждень 16	Комплексна перевірка надійності коду та аналіз аномалій у поведінці програмних компонентів	*Тест №4* (*max 5 бали*)

Шкала оцінювання: національна та ECTS

За шкалою ECTS	За шкалою університету	За національною шкалою	
		Екзамен	Залік
A	90 – 100 (відмінно)	5 (відмінно)	Зараховано
B	85 – 89 (дуже добре)	4 (добре)	
C	75 – 84 (добре)		
D	70 – 74 (задовільно)	3 (задовільно)	
E	60 – 69 (достатньо)		
FX	35 – 59 (незадовільно – з можливістю повторного складання)	2 (незадовільно)	Не зараховано
F	1 – 34 (незадовільно – з обов'язковим повторним курсом)		

СПИСОК ДЖЕРЕЛ

Основна література

1. Лісовська Ю. Кібербезпека. Ризики та заходи. – К.: Кондор, 2019. – 272 с.
2. Євсеєв С. П., Мілов О. В., Остапов С. Е., Сєвєрінов О. В. Кібербезпека: Основи кодування та криптографії : навч. посіб. – Харків ; Львів : Новий Світ-2000, 2023. – 658 с.
3. Євсеєв С. П., Шматко О. В., Король О. Г. Кібербезпека: криптографія з PYTHON : навч. посіб. / відп. ред. С. П. Євсеєв. – Харків ; Львів : Новий Світ-2000, 2021. – 119 с.
4. Євсеєв С. П., Мілов О. В., Король О. Г. Кібербезпека: лабораторний практикум з основ криптографічного захисту : навч. посіб. – Харків ; Львів : Новий Світ-2000, 2020. – 240 с.
5. Ковтун В. Ю., Євсеєв С. П., Аксьонова І. В. Кібербезпека та новітні технології захисту інформації : навч. посіб. – Харків : НТУ «ХПІ» ; Львів : Новий Світ-2000, 2024. – 284 с.

Допоміжна література

6. Євсеєв С. П., Ткачов А. М., Алексієв В. О., Рябуха Ю. М. Кібербезпека: WEB-технології : навч.-довід. посіб. – Львів : Новий Світ-2000, 2022. – 420 с.
7. Аналіз кіберзахищеності інформаційних систем : монографія / М. М. Браіловський та ін. – Київ : ФОП Ямчинський О. В., 2021. – 359 с.
8. Хорошко В. О. та ін. Захист систем електронних комунікацій : навч. посіб. – Київ : КНТЕУ, 2019. – 163 с.
9. Інформаційна безпека та інформаційні технології : монографія / за заг. ред. В. С. Пономаренка. – Харків : Діса плюс, 2019. – 321 с.
10. Євсеєв С. П., Остапов С. Е., Король О. Г. Кібербезпека: сучасні технології захисту : навч. посіб. – Львів : Новий Світ-2000, 2019. – 678 с.
11. Лісовська Ю. Кібербезпека. Ризики та заходи : навч. посіб. – Київ : Кондор, 2019. – 272 с.

Інформаційні ресурси та нормативно-правове забезпечення

12. Титова Н. М. та ін. Інформаційна безпека та кібербезпека держави : навч. посіб. – Київ : Ліра-К, 2025. – 223 с.
13. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII (зі змінами від 28.07.2022 р.). Відомості Верховної Ради України. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19

РЕГУЛЯЦІЇ І ПОЛІТИКИ КУРСУ[1]

Відвідування занять. Регуляція пропусків.
Інтерактивний характер курсу передбачає обов'язкове відвідування практичних занять. Аспіранти, які за певних обставин не можуть відвідувати практичні заняття регулярно, мусять впродовж тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущенні завдання мають бути відпрацьовані на найближчій консультації впродовж тижня після пропуску. Відпрацювання занять здійснюється шляхом виконання індивідуального письмового завдання. Аспіранти, які станом на початок екзаменаційної сесії мають понад 70% невідпрацьованих пропущених занять, до сесії не допускаються.

Політика академічної доброчесності
Усі письмові роботи, що виконуються аспірантами під час проходження курсу, перевіряються на наявність плагіату за допомогою спеціалізованого програмного забезпечення UniCheck. Відповідно до чинних правових норм, плагіатом вважатиметься: копіювання чужої наукової роботи чи декількох робіт та оприлюднення результату під своїм іменем; створення суміші власного та запозиченого тексту без належного цитування джерел; рерайт (перефразування чужої праці без згадування автора оригінального тексту). Будь-яка ідея, думка чи речення, ілюстрація чи фото, яке ви запозичуєте, має супроводжуватися посиланням на першоджерело. Приклади оформлення цитувань див. на платформі Moodle: https://cutt.ly/1I4Q8Me.
Виконавці індивідуальних завдань обов'язково додають до текстів своїх робіт власноруч підписану Декларацію академічної доброчесності (див. посилання у Додатку до силабусу).
Роботи, в яких виявлено ознаки плагіату, до розгляду не приймаються і відхиляються без права перескладання. Якщо ви не впевнені, чи підпадають зроблені вами запозичення під визначення плагіату, будь ласка, проконсультуйтеся з викладачем.
Висока академічна культура та європейські стандарти якості освіти, яких дотримуються в ЗНУ, вимагають від дослідників відповідального ставлення до вибору джерел. Посилання на такі ресурси, як Wikipedia, бази даних рефератів та письмових робіт (Studopedia.org та подібні) є неприпустимим. Рекомендовані бази даних для пошуку джерел: електронні ресурси Національної бібліотеки ім. Вернадського: http://www.nbuv.gov.ua; *наукометрична база Scopus: https://www.scopus.com; наукометрична база Web of Science: https://apps.webofknowledge.com*

Використання комп'ютерів/телефонів на занятті
Використання мобільних телефонів, планшетів та інших гаджетів під час лекційних та практичних занять дозволяється виключно у навчальних цілях (для уточнення певних даних, перевірки правопису, отримання довідкової інформації тощо). Будь ласка, не забувайте активувати режим «без звуку» до початку заняття.

Комунікація
Базовою платформою для комунікації викладача з аспірантами є платформа Moodle. Важливі повідомлення загального характеру регулярно розміщуються викладачем на форумі курсу. Для персональних запитів використовується сервіс приватних повідомлень. Відповіді на запити аспірантів подаються викладачем впродовж трьох робочих днів. Для оперативного отримання повідомлень про оцінки та нову інформацію, розміщену на платформі Moodle, будь ласка, переконайтеся, що адреса електронної пошти, зазначена у вашому профайлі на Moodle, є актуальною, та регулярно перевіряйте папку «Спам». Якщо за технічних причин доступ до Moodle є неможливим або ваше питання потребує термінового розгляду, направте електронного листа на пошту або у зазначені меседжери викладача. У листі обов'язково вкажіть ваше прізвище, ім'я та курс.

---

[1] Тут зазначається все, що важливо для курсу: наприклад, умови допуску до лабораторій, реактивів і т.д. Викладач сам вирішує, що треба знати студенту для успішного проходження курсу!

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
Силабус навчальної дисципліни

ДОДАТОК ДО СИЛАБУСУ ЗНУ

АКАДЕМІЧНА ДОБРОЧЕСНІСТЬ. Аспіранти і викладачі Запорізького національного університету несуть персональну відповідальність за дотримання принципів академічної доброчесності, затверджених ***Кодексом академічної доброчесності ЗНУ*****:** https://tinyurl.com/ya6yk4ad. *Декларація академічної доброчесності здобувача вищої освіти* (додається в обов'язковому порядку до письмових кваліфікаційних робіт, виконаних здобувачем, та засвідчується особистим підписом): https://tinyurl.com/y6wzzlu3.

ОСВІТНІЙ ПРОЦЕС ТА ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОСВІТИ. Перевірка набутих аспірантами знань, навичок та вмінь (атестації, заліки, іспити та інші форми контролю) є невід'ємною складовою системи забезпечення якості освіти і проводиться відповідно до *Положення про організацію та методику проведення поточного та підсумкового семестрового контролю навчання студентів ЗНУ*: https://tinyurl.com/y9tve4lk**.**

ПОВТОРНЕ ВИВЧЕННЯ ДИСЦИПЛІН, ВІДРАХУВАННЯ. Наявність академічної заборгованості до 6 навчальних дисциплін (в тому числі проходження практики чи виконання курсової роботи) за результатами однієї екзаменаційної сесії є підставою для надання аспіранту права на повторне вивчення зазначених навчальних дисциплін. Порядок повторного вивчення визначається *Положенням про порядок повторного вивчення навчальних дисциплін та повторного навчання у ЗНУ*: https://tinyurl.com/y9pkmmp5. Підстави та процедури відрахування аспірантів, у тому числі за невиконання навчального плану, регламентуються *Положенням про порядок переведення, відрахування та поновлення студентів у ЗНУ*: https://tinyurl.com/ycds57la.

НЕФОРМАЛЬНА ОСВІТА. Порядок зарахування результатів навчання, підтверджених сертифікатами, свідоцтвами, іншими документами, здобутими поза основним місцем навчання, регулюється *Положенням про порядок визнання результатів навчання, отриманих у неформальній освіті*: https://tinyurl.com/y8gbt4xs.

ВИРІШЕННЯ КОНФЛІКТІВ. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, регламентуються *Положенням про порядок і процедури вирішення конфліктних ситуацій у ЗНУ*: https://tinyurl.com/ycyfws9v. Конфліктні ситуації, що виникають у сфері стипендіального забезпечення здобувачів вищої освіти, вирішуються стипендіальними комісіями факультетів, коледжів та університету в межах їх повноважень, відповідно до: *Положення про порядок призначення і виплати академічних стипендій у ЗНУ*: https://tinyurl.com/yd6bq6p9; *Положення про призначення та виплату соціальних стипендій у ЗНУ*: https://tinyurl.com/y9r5dpwh.

ЗАПОБІГАННЯ КОРУПЦІЇ. Уповноважена особа з питань запобігання та виявлення корупції (Воронков В. В., 1 корп., 29 каб., тел. +38 (061) 289-14-18).

ПСИХОЛОГІЧНА ДОПОМОГА. Телефон довіри практичного психолога (061)228-15-84 (щоденно з 9 до 21).

РІВНІ МОЖЛИВОСТІ ТА ІНКЛЮЗИВНЕ ОСВІТНЄ СЕРЕДОВИЩЕ. Центральні входи усіх навчальних корпусів ЗНУ обладнані пандусами для забезпечення доступу осіб з інвалідністю та інших маломобільних груп населення. Допомога для здійснення входу у разі потреби надається черговими охоронцями навчальних корпусів. Якщо вам потрібна спеціалізована допомога, будь-ласка, зателефонуйте (061) 228-75-11 (начальник охорони). Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення у ЗНУ: https://tinyurl.com/ydhcsagx.

РЕСУРСИ ДЛЯ НАВЧАННЯ. Наукова бібліотека: http://library.znu.edu.ua. Графік роботи абонементів: понеділок – п`ятниця з 08.00 до 17.00; субота з 09.00 до 15.00.

ЕЛЕКТРОННЕ ЗАБЕЗПЕЧЕННЯ НАВЧАННЯ (MOODLE): HTTPS://MOODLE.ZNU.EDU.UA
Якщо забули пароль/логін, направте листа з темою «Забув пароль/логін» за адресами:
· для аспірантів ЗНУ - moodle.znu@gmail.com, Савченко Тетяна Володимирівна
У листі вкажіть: прізвище, ім'я, по-батькові українською мовою; шифр групи; електронну адресу.
Якщо ви вказували електронну адресу в профілі системи Moodle ЗНУ, то використовуйте посилання для відновлення паролю https://moodle.znu.edu.ua/mod/page/view.php?id=133015.

Центр інтенсивного вивчення іноземних мов: http://sites.znu.edu.ua/child-advance/
Центр німецької мови, партнер Гете-інституту: https://www.znu.edu.ua/ukr/edu/ocznu/nim
Школа Конфуція (вивчення китайської мови): http://sites.znu.edu.ua/confucius.