

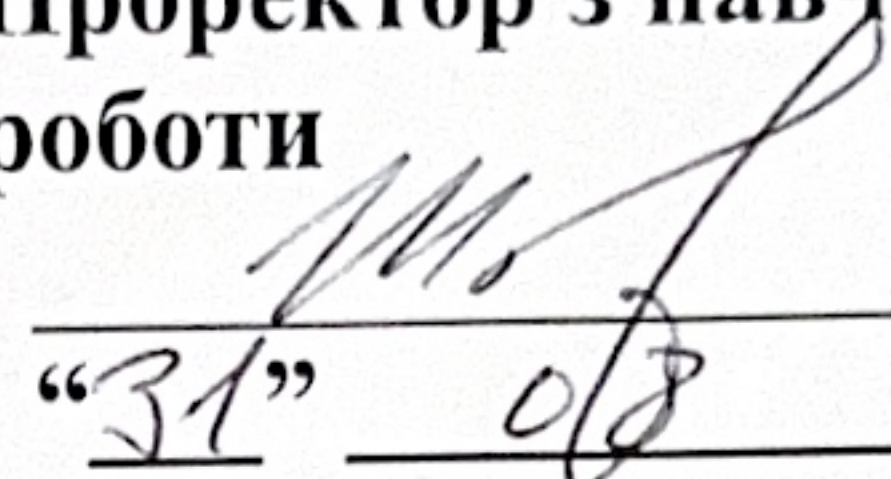
ЗАКЛАД ВИЩОЇ ОСВІТИ  
«УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА»

Факультет суспільних і прикладних наук

Кафедра інформаційних технологій

ЗАТВЕРДЖУЮ

Проректор з навчально-методичної  
роботи

 Ярослав ШТАНЬКО  
“31” 08 2026 р.

**БЕЗПЕКА ПРОГРАМ ТА ДАНИХ**

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

|                                                    |                                                    |
|----------------------------------------------------|----------------------------------------------------|
| Галузь знань:                                      | 12 Інформаційні технології                         |
| Спеціальність                                      | 121 Інженерія програмного забезпечення             |
| Освітньо-професійна<br>(освітньо-наукова) програма | Розробка та тестування<br>програмного забезпечення |
| Освітній рівень:                                   | перший (бакалаврський)                             |
| Статус дисципліни:                                 | вибіркова                                          |
| Мова викладання, навчання та<br>оцінювання:        | українська                                         |
| Семестр викладання                                 | VII                                                |

Івано-Франківськ

2026

РОЗРОБНИК:  
доцент кафедри

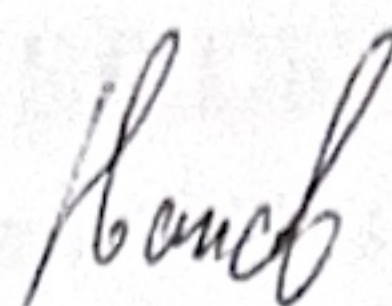


Тарас СТИСЛО

ЗАТВЕРДЖЕНО:

на засіданні кафедри інформаційних технологій, протокол № 1 від 27.08.2026 р.

PhD, завідувач кафедри



Олександр ІВАНОВ

УЗГОДЖЕНО:

Гарант ОП

к. ф-м.н., доцент кафедри



Володимир МАКОВИШИН

СХВАЛЕНО:

на засіданні Науково-методичної ради, протокол № 1 від 31 серпня 2026 року

|                            |                                                                                                                   |
|----------------------------|-------------------------------------------------------------------------------------------------------------------|
| e-mail                     | <a href="mailto:taras.styslo@ukd.edu.ua">taras.styslo@ukd.edu.ua</a>                                              |
| Номер аудиторії чи кафедри | Кафедра інформаційних технологій, ауд. 206                                                                        |
| Посилання на сайт          | <a href="https://ukd.edu.ua">https://ukd.edu.ua</a>                                                               |
| Сторінка курсу в СДО       | <a href="https://online.ukd.edu.ua/course/view.php?id=9141">https://online.ukd.edu.ua/course/view.php?id=9141</a> |

## ВСТУП

**Анотація.** Навчальна дисципліна «Безпека програм та даних» спрямована на формування у здобувачів освіти сучасного розуміння принципів безпечного проєктування, розроблення, тестування та експлуатації програмного забезпечення. Особлива увага приділяється практичним аспектам забезпечення безпеки програмних систем, виявленню та усуненню вразливостей, захисту даних, управлінню доступом, безпеці API та залежностей, а також сучасним ризикам, пов'язаним із використанням технологій штучного інтелекту.

Дисципліна орієнтована на підготовку майбутніх інженерів програмного забезпечення, здатних враховувати вимоги безпеки на всіх етапах життєвого циклу програмного продукту.

**Метою** дисципліни є формування у здобувачів освіти теоретичних знань і практичних навичок щодо розроблення безпечного програмного забезпечення, захисту даних, виявлення та мінімізації кіберризиків, а також інтеграції принципів безпеки в життєвий цикл розроблення програмних систем.

Для досягнення мети передбачається виконання таких **завдань**:

1. Сформувані розуміння основних понять, принципів і моделей безпеки програмного забезпечення та даних.
2. Ознайомити з принципами Secure Software Development Lifecycle (SSDLC), Security by Design, Shift Left Security, Defense in Depth та Least Privilege.
3. Навчити аналізувати архітектуру програмних систем, визначати поверхню атаки, моделювати загрози та оцінювати ризики.
4. Сформувані навички виявлення та усунення типових вразливостей вебзастосунків і API, зокрема відповідно до рекомендацій OWASP.
5. Ознайомити з сучасними підходами до автентифікації, авторизації та управління доступом, зокрема JWT, OAuth, OpenID Connect, MFA, RBAC та ABAC.
6. Навчити застосовувати методи захисту конфіденційних даних, паролів, ключів, токенів та інших секретів програмних систем.
7. Сформувані розуміння безпеки програмних залежностей та ланцюга постачання ПЗ, використання SAST, DAST, SCA, SBOM та засобів автоматизованого аналізу безпеки.
8. Ознайомити із сучасними ризиками використання ШІ у процесах розроблення програмного забезпечення та з особливостями захисту AI/LLM-систем.
9. Розвинути здатність приймати інженерні рішення, у яких безпека розглядається як невід'ємна характеристика програмного продукту.

У результаті вивчення дисципліни здобувач повинен **знати**:

- основні поняття інформаційної та програмної безпеки: asset, threat, vulnerability, exploit, attack surface, risk;

- принципи конфіденційності, цілісності та доступності даних;
- принципи Security by Design, Secure by Default, Least Privilege, Defense in Depth;
- структуру та принципи Secure Software Development Lifecycle;
- основи моделювання загроз та модель STRIDE;
- основні класи вразливостей вебзастосунків та API;
- принципи безпечної автентифікації й авторизації;
- принципи роботи JWT, OAuth, OpenID Connect, MFA, RBAC та ABAC;
- основні підходи до шифрування, хешування, захисту паролів і управління секретами;
- принципи Secure Coding та безпечної роботи із зовнішніми бібліотеками і залежностями;
- призначення SAST, DAST, SCA, secret scanning, dependency scanning та SBOM;
- основи безпеки CI/CD та програмного supply chain;
- основні загрози, пов'язані з AI-generated code, LLM, RAG та AI-агентами, зокрема Prompt Injection і витік конфіденційних даних.

У результаті вивчення дисципліни здобувач повинен **уміти**:

- аналізувати програмну систему з погляду потенційних загроз і вразливостей;
- визначати критичні активи та поверхню атаки програмної системи;
- створювати базову модель загроз і застосовувати STRIDE;
- оцінювати ризики та визначати пріоритетність їх усунення;
- виявляти типові вразливості вебзастосунків та API;
- аналізувати фрагменти програмного коду на предмет потенційних проблем безпеки;
- застосовувати принципи безпечної автентифікації, авторизації та контролю доступу;
- правильно організовувати зберігання паролів, токенів, API-ключів та інших секретів;
- використовувати сучасні засоби автоматизованого аналізу безпеки програмного забезпечення;
- аналізувати безпеку сторонніх бібліотек, пакетів та програмних залежностей;
- інтегрувати базові security-перевірки у процеси розроблення та CI/CD;
- визначати ризики використання генеративного ШІ під час розроблення програмного забезпечення;
- проєктувати програмні рішення з урахуванням вимог безпеки ще до початку їх реалізації.

У підсумку дисципліна має сформувати у студента підхід: безпека - це не окремий етап після завершення розроблення, а складова всього життєвого циклу програмного продукту.

### ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

|                                    |                        |                           |                            |
|------------------------------------|------------------------|---------------------------|----------------------------|
| <b>Курс</b>                        | <b>4</b>               |                           |                            |
| <b>Семестр</b>                     | <b>7</b>               |                           |                            |
| <b>Кількість кредитів ЄКТС</b>     | <b>6</b>               |                           |                            |
| <b>Аудиторні навчальні заняття</b> |                        | <b>денна<br/>форма</b>    | <b>заочна форма</b>        |
|                                    | лекції                 | <b>10<br/>(в годинах)</b> | <b>2<br/>(в годинах)</b>   |
|                                    | семінари,<br>практичні | <b>74<br/>(в годинах)</b> | <b>14<br/>(в годинах)</b>  |
| <b>Самостійна робота</b>           |                        | <b>96<br/>(в годинах)</b> | <b>164<br/>(в годинах)</b> |
| <b>Форма підсумкового контролю</b> | <b>екзамен</b>         |                           |                            |

### ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Перелік тем лекційного матеріалу

## **Тема 1. Безпека програмного забезпечення та Secure Software Development Lifecycle (SSDLC). (2 год.)**

Security by Design; Shift Left Security; моделі загроз; attack surface; assets/threats/vulnerabilities/risks; STRIDE; принцип найменших привілеїв; Defense in Depth; безпека на етапах Requirements → Design → Development → Testing → Deployment.

*Завдання для самостійної роботи.* Zero Trust Architecture та принципи Secure by Default у сучасних програмних системах. Методи оцінювання, класифікації та пріоритизації ризиків безпеки програмного забезпечення. NIST Secure Software Development Framework (SSDF) та OWASP Software Assurance Maturity Model (SAMM). Security Requirements, Trust Boundaries та Data Flow Diagrams (DFD) у процесі проектування безпечних програмних систем. DevSecOps та розподіл відповідальності за безпеку між учасниками життєвого циклу розробки програмного забезпечення. (16 год).

## **Тема 2. Уразливості вебзастосунків: як атакують сучасні системи. (2 год.)**

OWASP Top 10; SQL Injection; XSS; CSRF; SSRF; Path Traversal; Command Injection; insecure file upload; broken access control; демонстрація уразливий код → атака → виправлення.

*Завдання для самостійної роботи.* OWASP Top 10 як стандарт класифікації основних ризиків безпеки сучасних вебзастосунків. Ін'єкційні атаки у вебзастосунках: SQL Injection, Command Injection та методи їх запобігання. Атаки на клієнтську частину вебзастосунків: XSS, CSRF та сучасні механізми захисту. SSRF, Path Traversal та небезпечне завантаження файлів (Insecure File Upload): причини виникнення, наслідки та способи захисту. Broken Access Control та IDOR/BOLA: типові помилки контролю доступу та принципи побудови безпечної авторизації у вебзастосунках. (20 год).

## **Тема 3. Автентифікація, авторизація та управління доступом. (2 год.)**

Authentication vs Authorization; sessions; cookies; JWT; OAuth 2.0; OpenID Connect; MFA/2FA; RBAC/ABAC; password hashing; bcrypt/Argon2; brute-force protection; rate limiting; типові помилки JWT та access control.

*Завдання для самостійної роботи.* Сучасні методи багатофакторної автентифікації (MFA/2FA), Passkeys та безпарольна автентифікація. Безпечне управління сесіями та cookies у вебзастосунках: Secure, HttpOnly, SameSite та захист сесій. JWT: структура, принцип роботи, зберігання токенів та типові вразливості під час їх використання. OAuth 2.0 та OpenID Connect: принципи роботи, сценарії

використання та ризики неправильної конфігурації. Моделі управління доступом RBAC та ABAC, принцип найменших привілеїв і захист від Broken Access Control. (20 год).

#### **Тема 4. Захист даних та секретів у програмних системах. (2 год.)**

Data at Rest / Data in Transit; HTTPS/TLS; hashing vs encryption; symmetric/asymmetric encryption; AES/RSA/ECC на концептуальному рівні; password hashing; salts; API keys; .env; Secrets Management; резервне копіювання; мінімізація даних.

*Завдання для самостійної роботи.* Сучасні алгоритми симетричного та асиметричного шифрування: AES, RSA, ECC та сфери їх практичного застосування. HTTPS/TLS та цифрові сертифікати: принципи забезпечення захищеної передачі даних у мережі. Безпечне зберігання паролів: хешування, salt, bcrypt, Argon2 та типові помилки розробників. Secrets Management: безпечне зберігання API-ключів, токенів, паролів та інших секретів програмних систем. Захист життєвого циклу даних: мінімізація даних, резервне копіювання, контроль доступу та безпечне видалення інформації. (20 год).

#### **Тема 5. Безпека коду, API та Supply Chain Security. (2 год.)**

Secure Coding; input validation; dependency vulnerabilities; npm/pip/Maven packages; CVE/CVSS; SAST/DAST/SCA; dependency scanning; SBOM; secrets у Git; Docker/container security; CI/CD security; dependency confusion; typosquatting.

*Завдання для самостійної роботи.* Принципи Secure Coding та методи безпечної валідації й обробки вхідних даних у програмних системах. Вразливості програмних залежностей: CVE, CVSS, dependency scanning та безпечне використання npm, pip і Maven-пакетів. Методи автоматизованого аналізу безпеки програмного забезпечення: SAST, DAST, SCA та їх інтеграція у процес розробки. Software Supply Chain Security: SBOM, Dependency Confusion, Typosquatting та ризики використання сторонніх компонентів. Безпека Git, Docker та CI/CD: захист секретів, сканування контейнерів і побудова безпечного процесу доставки програмного забезпечення. (20 год).

### **Перелік тем практичного матеріалу**

## **«Аналіз та забезпечення безпеки програмної системи за темою кваліфікаційної роботи освітнього ступеня «бакалавр»»**

**Завдання проєкту:** упродовж семестру здобувачі освіти виконують комплексний проєкт із аналізу та забезпечення безпеки програмного продукту, що розробляється в межах їхньої кваліфікаційної роботи освітнього ступеня «бакалавр». Проєкт виконується поетапно відповідно до тематики практичних занять та передбачає застосування принципів Secure Software Development Lifecycle (SSDLC), моделювання загроз, аналіз уразливостей, реалізацію механізмів автентифікації та авторизації, захист даних, аналіз безпеки програмного коду, API та сторонніх залежностей.

### **Тема 1. Аналіз архітектури та активів програмної системи. (6 год.)**

Описати призначення та архітектуру програмного продукту за темою кваліфікаційної роботи. Визначити основні компоненти, користувачів, зовнішні сервіси, потоки даних та критичні активи (Assets), що потребують захисту.

### **Тема 2. Визначення Attack Surface та моделювання потоків даних. (6 год.)**

Побудувати Data Flow Diagram (DFD), визначити точки входу до системи, зовнішні інтерфейси, API, Trust Boundaries та сформулювати перелік потенційних точок атаки.

### **Тема 3. Моделювання загроз програмної системи за STRIDE. (8 год.)**

Провести Threat Modeling програмного продукту із застосуванням STRIDE. Визначити потенційні загрози, пов'язані зі Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service та Elevation of Privilege.

### **Тема 4. Оцінювання та пріоритизація ризиків безпеки. (6 год.)**

Для визначених загроз оцінити ймовірність реалізації та потенційний вплив. Сформулювати Risk Matrix, визначити критичні ризики та запропонувати заходи щодо їх мінімізації.

### **Тема 5. Аналіз програмного продукту відповідно до OWASP Top 10. (6 год.)**

Провести аналіз системи на наявність типових вразливостей вебзастосунків. Перевірити обробку вхідних даних, контроль доступу, конфігурацію системи, роботу з файлами та API.

**Тема 6. Аналіз та реалізація безпечної автентифікації й авторизації. (6 год.)**

Проаналізувати механізми Authentication та Authorization. Визначити ролі та права користувачів, сформуванати модель доступу RBAC/ABAC, перевірити безпеку сесій, cookies, JWT та механізмів відновлення доступу.

**Тема 7. Забезпечення захисту даних та секретів програмної системи. (8 год.)**

Визначити конфіденційні дані та секрети системи. Проаналізувати Data at Rest/Data in Transit, зберігання паролів, API keys і токенів. Передбачити використання HTTPS/TLS, hashing, encryption та Secrets Management.

**Тема 8. Аналіз безпеки програмного коду та API. (8 год.)**

Провести аналіз коду та API на потенційні проблеми безпеки. Перевірити input validation, error handling, access control, передачу конфіденційної інформації. Застосувати доступні засоби SAST/DAST та задокументувати результати.

**Тема 9. Аналіз програмних залежностей та Supply Chain Security. (8 год.)**

Проаналізувати сторонні бібліотеки та пакети (npm/pip/Maven тощо), виконати dependency scanning/SCA, перевірити відомі CVE та рівні CVSS, проаналізувати репозиторій на наявність секретів та оцінити ризики програмного ланцюга постачання.

**Тема 10. Комплексний аудит безпеки та захист семестрового проєкту. (12 год.)**

Провести повторний аналіз програмної системи після впровадження заходів захисту. Порівняти початковий і кінцевий стан безпеки, сформуванати підсумковий Security Report та презентувати реалізовані механізми захисту.

### Зміст самостійної роботи студентів

#### Розподіл годин, виділених на вивчення дисципліни «Безпека програм та даних»

| Найменування видів робіт                                 | Розподіл годин |              |
|----------------------------------------------------------|----------------|--------------|
|                                                          | Денна форма    | Заочна форма |
| <b>Самостійна робота, год, у т.ч.:</b>                   | <b>96</b>      | <b>164</b>   |
| Опрацювання матеріалу, викладеного на лекціях            | 10             | 90           |
| Підготовка до практичних занять та контрольних заходів   | 37             | 30           |
| Підготовка звітів з практичних робіт                     | 18             | 0            |
| Підготовка до поточного тестування                       | 12             | 14           |
| Опрацювання матеріалу, винесеного на самостійне вивчення | 19             | 30           |

### ПОЛІТИКА КУРСУ

#### 1) щодо системи поточного і підсумкового контролю

Організація поточного та підсумкового семестрового контролю знань студентів, проведення практик та атестації, переведення показників академічної успішності за 100-бальною шкалою в систему оцінок за національною шкалою здійснюється згідно з “Положенням про систему поточного і підсумкового контролю, оцінювання знань та визначення рейтингу здобувачів освіти”. Ознайомитись з документом можна за [покликанням](#).



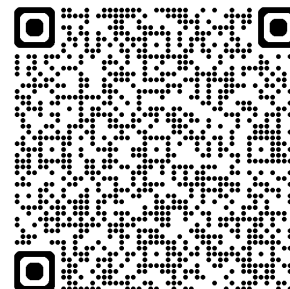
#### 2) щодо оскарження результатів контрольних заходів

Здобувачі вищої освіти мають право на оскарження оцінки з дисципліни отриманої під час контрольних заходів. Апеляція здійснюється відповідно до «Положення про політику та врегулювання конфліктних ситуацій». Ознайомитись з документом можна за [покликанням](#).



### 3) щодо відпрацювання пропущених занять

Згідно “Положення про організацію освітнього процесу” здобувач допускається до семестрового контролю з **конкретної навчальної дисципліни (семестрового екзамену, диференційованого заліку)**, якщо він виконав усі види робіт, передбачені на семестр навчальним планом та силабусом/робочою програмою навчальної дисципліни, підтвердив опанування на мінімальному рівні результатів навчання (отримав  $\geq 35$  бали), відпрацював визначені індивідуальним навчальним планом всі лекційні, практичні, семінарські та лабораторні заняття, на яких він був відсутній. Ознайомитись з документом можна за [покликанням](#).



### 4) щодо дотримання академічної доброчесності

“Положення про систему забезпечення академічної доброчесності” закріплює моральні принципи, норми та правила етичної поведінки, позитивного, сприятливого, доброчесного освітнього і наукового середовища, професійної діяльності та професійного спілкування спільноти Університету, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання. Ознайомитись з документом можна за [покликанням](#).



### 5) щодо використання штучного інтелекту

“Політика використання штучного інтелекту” визначає політику щодо використання технічних засобів на основі штучного інтелекту освітньому процесі. Ознайомитись з документом можна за [покликанням](#).<sup>1</sup> “Положення про систему забезпечення академічної доброчесності” містить рекомендації щодо використання в академічних текстах генераторів на основі штучного інтелекту. Ознайомитись з документом можна за [покликанням](#).



6

Під час вивчення навчальної дисципліни «Нон-фікшн наратив» здобувачі використовують ШІ:

- 1) як інструментарій для генерації відео контенту за темою свого відео есе (якщо не вимагається оригінальна власна зйомка); генерації зображень для ілюстрації презентацій, візуалізацій до доповідей, до медійного контенту;
- 2) для опрацювання великих даних (кількісних та якісних);
- 3) для транскрибації інтерв'ю;
- 4) для створення субтитрів та перекладів тексту іншими мовами;
- 5) для драфт-скриптів;
- 6) голосовий супровід оригінального відео контенту;
- 7) очищення звуку, обробка відео та фото матеріалів.



<sup>1</sup> визначається політика використання ШІ в навчальній дисципліні - дозволене/забороне

### **6) щодо використання технічних засобів в аудиторії та правила комунікації**

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). На гаджетах повинен бути активований режим «без звуку» до початку заняття. Під час занять заборонено надсилання текстових повідомлень, прослуховування музики, перевірка електронної пошти, соціальних мереж тощо, окрім виробничої необхідності. Під час виконання заходів контролю використання гаджетів заборонено (за винятком, коли це передбачено умовами його проведення). У разі порушення цієї заборони результат анулюється без права перескладання. Ознайомитись з відповідним документом можна за [посиланням](#).

Комунікація відбувається через електронну пошту і сторінку дисципліни в Moodle.

### **7) щодо зарахування результатів навчання, здобутих шляхом формальної/інформальної освіти**

Процедури визнання результатів навчання, здобутих шляхом формальної/інформальної освіти визначаються «Положенням про порядок визнання результатів навчання, здобутих шляхом неформальної та / або інформальної освіти». Ознайомитись з документом можна за [посиланням](#).<sup>2</sup>

Під час вивчення навчальної дисципліни «Безпека програм та даних» студентам надається можливість перезарахування неформальної освіти. До прикладу, із запропонованого переліку можна пройти сертифіковані (безкоштовні) курси на освітніх платформах, відтак сертифікат, який отримали під час навчання, — є підтвердженням засвоєння студентом окремих тем, що включені у зміст дисципліни.



<sup>2</sup> зміст пунктів може редагуватись з огляду на особливості курсу

## МЕТОДИ НАВЧАННЯ

При вивченні дисципліни застосовується комплекс методів для організації навчання студентів з метою розвитку їх логічного та абстрактного мислення, творчих здібностей, підвищення мотивації до навчання та формування особистості майбутнього фахівця в галузі інформаційних технологій.

| Програмний результат навчання <sup>3</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Метод навчання                                                                                                                                                                                                   | Метод оцінювання                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| <p><b>ПРН 14</b> - Застосовувати на практиці інструментальні програмні засоби доменного аналізу, проектування, тестування, візуалізації, вимірювань та документування програмного забезпечення.</p> <p><b>ПРН 18</b> - Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних.</p> <p><b>ПРН 19</b> - Знати та вміти застосовувати методи верифікації та валідації програмного забезпечення.</p> <p><b>ПРН 21</b> - 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.</p> | <p>Лекція, розповідь-пояснення, бесіда, комп'ютерні і мультимедійні методи, практичні роботи, дедуктивний, порівняння, проблемно-пошуковий, дослідницький, робота під керівництвом викладача, бесіда-діалог.</p> | <p>Екзамен, поточний контроль, усний контроль, тестовий контроль.</p> |

<sup>3</sup> для вибіркових навчальних дисциплін вказується **результат навчання**

### ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

| Вид                          | Зміст   | % від загальної оцінки | Бал |     |
|------------------------------|---------|------------------------|-----|-----|
|                              |         |                        | min | max |
| Поточні контрольні заходи    | всього  | 60                     | 35  | 60  |
| Підсумкові контрольні заходи | екзамен | 40                     | 24  | 40  |
| Всього:                      | -       | 100                    | 60  | 100 |

Процедура проведення контрольних заходів, а саме поточного контролю знань протягом семестру та підсумкового семестрового контролю, регулюється «Положенням про систему поточного та підсумкового контролю оцінювання знань та визначення рейтингу студентів».

Фіксація **поточного** контролю здійснюється в “Електронному журналі обліку успішності академічної групи” на підставі чотирибальної шкали – “2”; “3”; “4”; “5”. У разі відсутності студента на занятті виставляється “н”. За результатами поточного контролю у Журналі, автоматично визначається підсумкова оцінка, здійснюється підрахунок пропущених занять.

***Критерії оцінювання (аудиторні заняття):***

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>«незадовільно»</b> | володіє навчальним матеріалом на рівні елементарного розпізнавання і відтворення окремих фактів, елементів, об’єктів, що позначаються окремими словами чи реченнями; володіє матеріалом на елементарному рівні засвоєння, викладає його уривчастими реченнями, виявляє здатність висловити думку на елементарному рівні; володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу; |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| «задовільно» | володіє матеріалом на початковому рівні, значну частину матеріалу відтворює на репродуктивному рівні; володіє матеріалом на рівні, вищому за початковий, здатний за допомогою викладача логічно відтворити значну його частину; може відтворити значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, за допомогою викладача може аналізувати навчальний матеріал, порівнювати та робити висновки, виправляти допущені помилки;                                                                                                                                                                                                                                                                                                                        |
| «добре»      | здатний застосовувати вивчений матеріал на рівні стандартних ситуацій, частково контролювати власні навчальні дії, наводити окремі власні приклади на підтвердження певних тверджень: вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, в цілому самостійно застосовувати її на практиці, контролювати власну діяльність, виправляти помилки і добирати аргументи на підтвердження певних думок під керівництвом викладача; вільно володіє вивченим обсягом матеріалу, та вміє застосовувати його на практиці; вільно розв'язує задачі в стандартних ситуаціях, самостійно виправляє допущені помилки, добирає переконливі аргументи на підтвердження вивченого матеріалу;                                                                      |
| «відмінно»   | виявляє початкові творчі здібності, самостійно визначає окремі цілі власної навчальної діяльності, оцінює окремі нові факти, явища, ідеї; знаходить джерела інформації та самостійно використовує їх відповідно до цілей, поставлених викладачем; вільно висловлює власні думки і відчуття, визначає програму особистої пізнавальної діяльності, самостійно оцінює різноманітні життєві явища і факти, виявляючи особисту позицію щодо них; без допомоги викладача знаходить джерела інформації і використовує одержані відомості відповідно до мети та завдань власної пізнавальної діяльності; використовує набуті знання і вміння в нестандартних ситуаціях; виявляє особливі творчі здібності, самостійно розвиває власні обдарування і нахили, вміє самостійно здобувати знання. |

**Критерії оцінювання (підсумковий контроль) для семестрового проєкту з дисципліни «Безпека програм та даних»:** оцінюється здатність здобувача комплексно аналізувати безпеку програмного продукту за темою власної кваліфікаційної роботи, визначати загрози та вразливості, оцінювати ризики, обґрунтовувати та реалізовувати механізми захисту, застосовувати сучасні методи й інструменти аналізу безпеки та презентувати результати проведеного аудиту.

|            |                                                                                                                                        |
|------------|----------------------------------------------------------------------------------------------------------------------------------------|
| «відмінно» | <b>Аналіз системи:</b> представлено повний та обґрунтований аналіз архітектури програмного продукту; коректно визначено Assets, Attack |
|------------|----------------------------------------------------------------------------------------------------------------------------------------|

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | <p>Surface, Trust Boundaries та потоки даних; побудовано DFD. Threat Modeling: проведено ґрунтовне моделювання загроз із використанням STRIDE, визначено та пріоритизовано ризики, сформовано Risk Matrix.</p> <p><b>Аналіз уразливостей:</b> проведено комплексний аналіз відповідно до OWASP Top 10; продемонстровано розуміння причин виникнення вразливостей та можливих сценаріїв атак.</p> <p><b>Реалізація захисту:</b> обґрунтовано та реалізовано механізми Authentication/Authorization, контролю доступу, захисту даних і секретів.</p> <p>Security Testing: використано сучасні засоби SAST/DAST/SCA, dependency та secret scanning; проаналізовано результати, CVE/CVSS та програмні залежності.</p> <p><b>Результат:</b> виявлені критичні проблеми усунено або запропоновано технічно обґрунтовані заходи їх мінімізації. Сформовано структурований Security Report із доказами проведеного аналізу.</p> <p><b>Захист:</b> студент аргументовано пояснює прийняті рішення, демонструє роботу реалізованих механізмів безпеки та впевнено відповідає на запитання. Дотримано академічної доброчесності, зазначено використані джерела, інструменти та засоби ШІ.</p> |
| <b>«добре»</b>      | <p><b>Аналіз системи:</b> архітектуру програмного продукту описано коректно, визначено основні Assets, Attack Surface та Trust Boundaries, однак окремі компоненти або потоки даних проаналізовано недостатньо детально. Threat Modeling: застосовано STRIDE та проведено оцінювання ризиків, проте частина потенційних загроз не врахована або їх пріоритизація недостатньо аргументована.</p> <p><b>Аналіз уразливостей:</b> проведено аналіз за OWASP Top 10 та використано інструменти автоматизованого security testing, але результати частково мають описовий характер.</p> <p><b>Реалізація захисту:</b> основні механізми Authentication/Authorization, захисту даних і секретів реалізовано правильно, проте присутні окремі недоліки.</p> <p><b>Результат:</b> більшість виявлених проблем усунено; сформовано Security Report, який містить основні результати роботи.</p> <p><b>Захист:</b> студент розуміє реалізовані рішення та відповідає на більшість запитань, однак окремі рішення пояснює недостатньо аргументовано.</p>                                                                                                                                      |
| <b>«задовільно»</b> | <p><b>Аналіз системи:</b> виконано базовий опис програмного продукту, однак архітектурна схема, Assets, Attack Surface або Trust Boundaries визначені частково. Threat Modeling: STRIDE використано формально; визначено лише очевидні загрози, оцінювання ризиків поверхневе.</p> <p><b>Аналіз уразливостей:</b> перевірено лише окремі категорії OWASP Top 10; результати переважно отримані автоматизованими засобами без достатнього самостійного аналізу.</p> <p><b>Реалізація захисту:</b> наявні базові механізми автентифікації, авторизації та захисту даних, але вони реалізовані частково або містять недоліки.</p> <p>Security Testing: використано обмежену кількість інструментів; результати сканування наведені без належної інтерпретації.</p> <p><b>Результат:</b> частина виявлених проблем залишилася невирішеною, Security Report неповний або недостатньо структурований.</p>                                                                                                                                                                                                                                                                                |

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <b>Захист:</b> студент може пояснити загальні принципи роботи проєкту, але має труднощі з обґрунтуванням security-рішень та відповідями на запитання.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>«незадовільно»</b> | <p><b>Проект:</b> робота відсутня, не відповідає темі кваліфікаційної роботи або не демонструє виконання завдань дисципліни.</p> <p><b>Аналіз:</b> відсутні або некоректно виконані аналіз архітектури, визначення Assets/Attack Surface, Threat Modeling та оцінювання ризиків.</p> <p><b>Безпека:</b> не проведено аналіз OWASP Top 10, не реалізовано або принципово неправильно реалізовано базові механізми Authentication/Authorization та захисту даних. Security Testing: відсутні результати перевірки коду, API та програмних залежностей або наведено сторонні результати, що не стосуються розробленого продукту.</p> <p><b>Результат:</b> Security Report відсутній або має формальний характер і не підтверджує фактичного виконання роботи.</p> <p><b>Захист:</b> студент не може пояснити архітектуру власного програмного продукту, виявлені загрози, використані інструменти та реалізовані механізми захисту.</p> <p><b>Доброчесність:</b> виявлено плагіат, використання чужого проєкту або повністю автоматично згенерованих матеріалів/результатів без їх перевірки, розуміння та самостійного опрацювання студентом.</p> |

Студент повинен на захисті продемонструвати не тільки Security Report, а й сам програмний продукт, його код/репозиторій, результати security-сканування та щонайменше 2–3 реально впроваджені механізми захисту. Це суттєво зменшить можливість здати повністю згенерований III звіт без реальної роботи над бакалаврським проєктом.

Усі пропущені заняття, а також негативні оцінки студенти зобов'язані відпрацювати впродовж трьох наступних тижнів. У випадку недотримання цієї норми, замість “н” в журналі буде виставлено “0” (нуль балів), без права перездачі. Відпрацьоване лекційне заняття в електронному журналі позначається літерою «в».<sup>4</sup>

До підсумкового контролю допускаються студенти які за результатами поточного контролю отримали не менше 35 балів. Усі студенти, що отримали 34 балів і менше, не допускаються до складання підсумкового контролю і на підставі укладання додаткового договору, здійснюють повторне вивчення дисципліни впродовж наступного навчального семестру. За результатами підсумкового контролю (диференційований залік/екзамен) студент може отримати 40 балів. Студенти, які під час підсумкового контролю отримали 24 бали і менше, вважаються такими, що не здали екзамен/диференційований залік і повинні йти на перездачу.

<sup>4</sup> можна вказати теми чи завдання, які є обов'язковими до виконання, а також особисті підходи до оцінювання рівня знань здобувачів під час аудиторної роботи

Загальна семестрова оцінка з дисципліни, яка виставляється в екзаменаційних відомостях оцінюється в балах (згідно з **Шкалою оцінювання знань за ЄКТС**) і є сумою балів отриманих під час поточного та підсумкового контролю.

### **Шкала оцінювання знань за ЄКТС:**

| <b>Оцінка за національною шкалою</b>       | <b>Рівень досягнень, %</b> | <b>Шкала ECTS</b> |
|--------------------------------------------|----------------------------|-------------------|
| <b>Національна диференційована шкала</b>   |                            |                   |
| Відмінно                                   | 90 – 100                   | A                 |
| Добре                                      | 83 – 89                    | B                 |
|                                            | 75 – 82                    | C                 |
| Задовільно                                 | 67 – 74                    | D                 |
|                                            | 60 – 66                    | E                 |
| Незадовільно                               | 35 – 59                    | FX                |
|                                            | 0 – 34                     | F                 |
| <b>Національна недиференційована шкала</b> |                            |                   |
| Зараховано                                 | 60 – 100                   | -                 |
| Не зараховано                              | 0 – 59                     | -                 |

Студенти, які не з'явилися на екзамени без поважних причин, вважаються такими, що одержали незадовільну оцінку.

### **РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ<sup>5</sup>**

#### **Основна література**

1. Stallings W., Brown L. Computer Security: Principles and Practice. 5th ed. Pearson, 2023.
2. Janca T. Alice and Bob Learn Application Security. Indianapolis : Wiley, 2020. 288 p.

<sup>5</sup> рекомендовано використовувати літературу за останні 5-7 років, обов'язкове наведення власної публікації за змістом навчальної дисципліни

3. McDonald M. Web Security for Developers: Real Threats, Practical Defense. San Francisco : No Starch Press, 2020. 216 p.
4. Li V. Bug Bounty Bootcamp: The Guide to Finding and Reporting Web Vulnerabilities. San Francisco : No Starch Press, 2021. 416 p.
5. Seitz J., Arnold T. Black Hat Python: Python Programming for Hackers and Pentesters. 2nd ed. San Francisco : No Starch Press, 2021. 216 p.
6. Souppaya M., Scarfone K., Dodson D. Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. NIST Special Publication 800-218. Gaithersburg : National Institute of Standards and Technology, 2022. DOI: 10.6028/NIST.SP.800-218.
7. OWASP Foundation. OWASP Top 10:2025. The Ten Most Critical Web Application Security Risks [Електронний ресурс]. 2025. URL: [OWASP Top 10:2025](#) (дата звернення: 06.10.2026).
8. OWASP Foundation. OWASP Application Security Verification Standard (ASVS) [Електронний ресурс]. URL: [OWASP ASVS](#) (дата звернення: 06.10.2026).

### **Електронні інформаційні ресурси**

1. Open Worldwide Application Security Project (OWASP) [Електронний ресурс]. URL: [OWASP](#) (дата звернення: 30.08.2026).
2. OWASP Top 10:2025 [Електронний ресурс]. URL: [OWASP Top 10](#) (дата звернення: 30.08.2026).
3. OWASP Cheat Sheet Series [Електронний ресурс]. URL: [OWASP Cheat Sheet Series](#) (дата звернення: 30.08.2026).
4. OWASP Web Security Testing Guide (WSTG) [Електронний ресурс]. URL: [OWASP WSTG](#) (дата звернення: 30.08.2026).
5. OWASP API Security Project [Електронний ресурс]. URL: [OWASP API Security Project](#) (дата звернення: 30.08.2026).
6. OWASP Application Security Verification Standard (ASVS) [Електронний ресурс]. URL: [OWASP ASVS](#) (дата звернення: 30.08.2026).
7. NIST Secure Software Development Framework (SSDF) [Електронний ресурс]. National Institute of Standards and Technology. URL: [NIST SSDF](#) (дата звернення: 30.08.2026).
8. Web Security Academy [Електронний ресурс]. PortSwigger. URL: [PortSwigger Web Security Academy](#) (дата звернення: 30.08.2026).
9. CVE Program. Common Vulnerabilities and Exposures [Електронний ресурс]. URL: [CVE Program](#) (дата звернення: 30.08.2026).

10. National Vulnerability Database (NVD) [Электронный ресурс]. National Institute of Standards and Technology. URL: [NIST National Vulnerability Database](#) (дата звернения: 30.08.2026).
11. Common Vulnerability Scoring System (CVSS) [Электронный ресурс]. Forum of Incident Response and Security Teams. URL: [FIRST CVSS](#) (дата звернения: 30.08.2026).
12. GitHub Code Security Documentation [Электронный ресурс]. URL: [GitHub Code Security Documentation](#) (дата звернения: 30.08.2026).
13. Docker Security [Электронный ресурс]. Docker Documentation. URL: [Docker Security Documentation](#) (дата звернения: 30.08.2026).
14. Secure by Design [Электронный ресурс]. Cybersecurity and Infrastructure Security Agency. URL: [CISA Secure by Design](#) (дата звернения: 30.08.2026).