Національний транспортний університет

ВК Засоби захисту інформації

Рівень вищої освіти – *другий (магістерський)*

Дні занять, час занять, аудиторія: будуть доступні згідно розкладу за посиланням **https://kizt.ntu.edu.ua/to-the-student/rozklady-zanyat-i-sesij/**

Кафедра інформаційних технологій та штучного інтелекту

Лекції проводить
д.т.н., професор Ніконов Олег Якович

Контактна інформація	o.nikonov@ntu.edu.ua +380 (50) 750-50-10
Адреса, номер аудиторії	м. Київ, вул. Івана Огієнка, 19, каб. 601а
Час консультацій	Щовівторка з 10:00 до 11:00

Практичні заняття проводить

д.т.н., професор Ніконов Олег Якович

Контактна інформація	o.nikonov@ntu.edu.ua +380 (50) 750-50-10
Адреса, номер аудиторії	м. Київ, вул. Івана Огієнка, 19, каб. 601а
Час консультацій	Щовівторка з 10:00 до 11:00

Анотація курсу: дисципліна «Засоби захисту інформації» формує практичні вміння добирати, розгортати, налаштовувати та оцінювати програмні засоби захисту інформації. Основну увагу приділено інфраструктурі відкритих ключів і керуванню ключами, керуванню секретами, автоматизованому аналізу захищеності програмного забезпечення, формуванню SBOM, контролю залежностей, цілісності та безпечних конфігурацій.

Предметом вивчення навчальної дисципліни є методи практичного застосування, інтеграції та порівняльного оцінювання програмних засобів захисту інформації у процесах розроблення й експлуатації програмних систем. Обсяг дисципліни - 4 кредити ECTS (120 годин): денна форма - 18 годин лекцій, 18 годин практичних занять і 84 години самостійної роботи; заочна форма - 2 години лекцій, 4 години практичних занять і 114 годин самостійної роботи.

Мета курсу: сформувати здатність обґрунтовано обирати й безпечно застосовувати засоби захисту інформації, перевіряти результативність їх налаштування та документувати отримані результати.

Очікувані результати навчання: після завершення курсу здобувач освіти зможе: 1) формувати технічні вимоги та критерії вибору засобів захисту; 2) розгортати відтворюване лабораторне середовище та безпечно працювати з тестовими даними; 3) створювати й перевіряти сертифікати, керувати життєвим циклом ключів і секретів; 4) виконувати SAST, DAST і SCA, формувати SBOM та опрацьовувати результати сканування; 5) перевіряти цілісність і відповідність конфігурацій

установленим базовим профілям; 6) порівнювати засоби за функціональністю, точністю, обмеженнями й вартістю впровадження та готувати обґрунтований звіт.

Міждисциплінарні зв'язки: дисципліна пов'язана з освітніми компонентами «Гібридні загрози та комплексна безпека», «Інформаційна безпека та гібридні загрози» та «Інноваційні технології Big Data та інформаційної безпеки в управлінні транспортними системами».

Програма навчальної дисципліни складається з таких модулів:

Модуль 1. Криптографічна інфраструктура та керування секретами

Тема 1. Лабораторне середовище й оцінювання засобів захисту

Безпечна робота в ізольованому середовищі. Інвентаризація активів і вимоги до засобу. Критерії порівняння: покриття, сумісність, точність, хибні спрацювання, журналювання, супроводжуваність і вартість. План перевірки, контрольні приклади та докази результативності.

Тема 2. PKI та засоби керування життєвим циклом ключів

Практичне використання OpenSSL і GnuPG: ключові пари, запити на сертифікат і локальний центр сертифікації. Перевірка ланцюжка довіри, строку дії та відкликання сертифікатів; підписування файлів. Генерування, зберігання, резервування, ротація, відкликання та знищення ключів. Призначення TPM і HSM.

Тема 3. Засоби керування секретами та політиками доступу

Централізоване зберігання секретів на прикладі HashiCorp Vault або сумісного засобу. Політики найменших привілеїв, токени, строк оренди, ротація та відкликання секретів. Статичні й динамічні облікові дані. Інтеграція із застосунком і CI/CD без розміщення секретів у вихідному коді. Аудит операцій і перевірка сценаріїв компрометації.

Модуль 2. Автоматизована перевірка захищеності програмних систем

Тема 4. Засоби статичного й динамічного аналізу захищеності

Призначення та межі SAST і DAST. Побудова набору правил та запуск статичного аналізу на прикладі Semgrep. Динамічна перевірка тестового вебзастосунку засобами OWASP ZAP. Налаштування контексту й автентифікованого сканування. Відтворення, класифікація та пріоритизація знахідок; аналіз хибних спрацювань. Формування технічного звіту й контроль усунення вразливостей.

Тема 5. Контроль компонентів, цілісності та безпечних конфігурацій

Формування SBOM у форматі CycloneDX. Аналіз сторонніх компонентів і відомих вразливостей засобами SCA та OWASP Dependency-Track. Перевірка контрольних сум, цифрових підписів артефактів і цілісності файлів. Базові профілі безпечної конфігурації та автоматизована перевірка на прикладі OpenSCAP. Порівняльне оцінювання інструментів і підготовка рекомендацій щодо їх інтеграції у процес розроблення програмного забезпечення.

Методи поточного контролю: виконання та захист практичних робіт, короткі тематичні тести, перевірка конфігурацій і звітів інструментів, усне обґрунтування вибору засобу захисту.

Методи модульного контролю: для денної форми - дві модульні контрольні роботи по 10 балів; для заочної форми - контрольна робота на 20 балів. Підсумковий контроль - 40 балів; його форму буде уточнено після визначення коду вибіркового компонента.

Основні джерела для вивчення дисципліни:

1. Методичні матеріали, інструкції та завдання до практичних робіт, розміщені у віртуальному середовищі навчання.
2. Електронний ресурс бібліотеки НТУ: http://lib.ntu.edu.ua/catalog/login.html

3. Віртуальне середовище навчання (Google Classroom): посилання на курс надається викладачем на першому занятті.

Оцінювання

Підсумкова оцінка за дисципліну становить не більше 100 балів: поточний і модульний контроль - 60 балів, підсумковий контроль - 40 балів.

<table>
<tr><td colspan="5">Контроль протягом семестру (60 балів)</td><td rowspan="2">Підсумковий контроль</td><td rowspan="2">Сума балів</td></tr>
<tr><td colspan="3">Модуль 1</td><td colspan="2">Модуль 2</td><td rowspan="2">Модуль 3 (ІЗ)</td></tr>
<tr><td>Тема 1</td><td>Тема 2</td><td>Тема 3</td><td>Тема 4</td><td>Тема 5</td></tr>
<tr><td colspan="5">Для денної форми: за кожною з тем 1–5 - до 6 балів за виконання і захист практичної роботи та до 2 балів за тематичний тест або усне обґрунтування.
модульні контрольні роботи по 10 балів
Разом за теми - 60 балів.</td><td>Не передбачено освітньою програмою та навчальним планом</td><td rowspan="2">40</td><td rowspan="2">100</td></tr>
<tr><td colspan="5">Для заочної форми: за кожною з тем 1–5 - до 8 балів за виконання і захист практичного завдання.
контрольна робота на 20 балів
Разом за теми - 60 балів.</td><td>Не передбачено освітньою програмою та навчальним планом</td></tr>
</table>

Самостійна робота

Самостійна робота охоплює підготовку середовища, опрацювання документації, завершення практичних завдань, аналіз сканувань та оформлення звітів.

Результати неформальної або інформальної освіти можуть бути визнані замість відповідних завдань за процедурою НТУ в межах 60 балів і не збільшують максимальну оцінку понад 100 балів.

Критерії оцінювання: відтворюваність налаштування; обґрунтованість вибору засобу; повнота перевірки; коректність аналізу знахідок і хибних спрацювань; якість доказів та звіту. Підсумкову оцінку визначають відповідно до Додатка 1 до Положення про організацію освітнього процесу в НТУ. http://vstup.ntu.edu.ua/pro_orhanizatsiyu_osvitnoho_protsesu.pdf

Політика несвоєчасного проходження контрольних заходів.

Поточний та підсумковий контролі проводяться згідно з графіком освітнього процесу та затвердженими графіками. У разі неявки на підсумковий контроль з поважної причини контроль може бути проведений індивідуально в погоджений строк за наявності дозволу дирекції ННКІЗТ.

Повторне складання підсумкового контролю в разі отримання незадовільної оцінки допускається не більше двох разів: один раз - викладачеві, другий - комісії, створеній директором ННКІЗТ відповідно до чинних нормативних документів НТУ.

У разі подання завдання пізніше встановленого строку без поважної причини оцінка знижується на 10 %. Документовані збої електронного середовища навчання, аварійні відключення або інші обставини, що об’єктивно унеможливили своєчасне подання, розглядаються викладачем індивідуально.

Політика перескладання. Упродовж тижня після оголошення результатів поточного контролю здобувач освіти може звернутися до викладача за роз’ясненням або з обґрунтованою незгодою. Апеляція щодо підсумкового контролю подається в порядку та строки, визначені чинними

нормативними документами НТУ. Повторне проходження підсумкового контролю з метою підвищення позитивної оцінки не допускається.

Політика відвідування та активності. Здобувач освіти має брати участь у заняттях і виконувати передбачені курсом завдання. Пропущені практичні роботи та контрольні заходи виконуються за погодженим індивідуальним графіком до завершення підсумкового контролю. Допуск ґрунтується на виконанні обов'язкових оцінюваних завдань, а не лише на факті відвідування.

Академічна доброчесність: регулюється Кодексом етики академічних взаємовідносин та доброчесності НТУ, Положенням про систему забезпечення академічної доброчесності та іншими чинними нормативними документами університету.
Порушеннями академічної доброчесності є:

- академічний плагіат;
- фальсифікація;
- списування;
- обман;
- неправомірна вигода;
- хабарництво.

Під час поточного або підсумкового контролю дозволено використовувати лише ті джерела й засоби, які прямо визначив викладач. Ознаки списування, недозволеної допомоги або підміни авторства розглядаються за процедурами академічної доброчесності НТУ.

Поведінка в аудиторії. Ноутбуки та портативні пристрої використовуються з навчальною метою відповідно до завдань курсу. Не допускається використання пристроїв, яке перешкоджає заняттю або порушує академічну доброчесність. Обмеження не поширюються на погоджені засоби доступності та допоміжні технології.
В аудиторії забороняється вживання їжі, напоїв (за винятком води). Здобувачі вищої освіти та викладачі повинні дотримуватися етичних норм поведінки.

Підтримка здобувачів з особливими освітніми потребами погоджується з дирекцією ННКІЗТ.

За проблем зі здоров'ям, що перешкоджають навчанню, здобувач звертається до медичного закладу та повідомляє дирекцію ННКІЗТ.

Скарги, пропозиції, зауваження та повідомлення про конфліктні ситуації в межах освітніх програм можна надсилати на електронну адресу general@ntu.edu.ua або через скриньку довіри, розміщену при вході до університету.

Електронна скринька для звернень до психологічної служби: philosophy@ntu.edu.ua.

Канали зв'язку з розробником силабуса:
o.nikonov@ntu.edu.ua ; +380 (50) 750-50-10.

Рекомендована література:
Основна:

1. NIST. The NIST Cybersecurity Framework (CSF) 2.0. 2024. URL: https://www.nist.gov/cyberframework.
2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. URL: https://www.iso.org/standard/27001.

3. Barker E. NIST SP 800-57 Part 1 Rev. 5. Recommendation for Key Management: Part 1 - General. 2020. URL: https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final.
4. NIST. SP 800-218. Secure Software Development Framework (SSDF) Version 1.1. 2022. URL: https://csrc.nist.gov/pubs/sp/800/218/final.

Додаткова:

5. OWASP. Application Security Verification Standard 5.0.0. URL: https://owasp.org/www-project-application-security-verification-standard/.
6. OpenSSL Project. OpenSSL Documentation. URL: https://docs.openssl.org/.
7. HashiCorp. Vault Documentation. URL: https://developer.hashicorp.com/vault/docs.
8. OWASP. ZAP Documentation. URL: https://www.zaproxy.org/docs/.
9. Semgrep. Documentation. URL: https://semgrep.dev/docs/.
10. OWASP. Dependency-Track: Software Composition Analysis and SBOM Platform. URL: https://owasp.org/www-project-dependency-track/.
11. OpenSCAP. Security Compliance and Configuration Scanning Tools. URL: https://www.open-scap.org/.

Додаткова інформація

Детальнішу інформацію щодо методів навчання, практичних занять, форм оцінювання, самостійної роботи та повного списку літератури наведено у Робочій програмі навчальної дисципліни.