



**ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ  
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

Кафедра кібербезпеки та програмного забезпечення



**СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

**БЕЗПЕКА БАЗ ДАНИХ**

першого рівня вищої освіти

м. Кропивницький

## 1. Загальна інформація

Назва дисципліни	<b>Безпека баз даних</b>
Викладач	Лектор – Буравченко Костянтин Олегович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та програмного забезпечення
Контактний телефон	службовий: (0522)390-449 – робочі дні з 8 <sup>30</sup> до 14 <sup>20</sup>
E-mail:	buravchenkoko@kntu.kr.ua
Консультації	<i>Очні консультації</i> відповідно до затвердженого графіку консультацій <i>Онлайн консультації</i> засобами електронної пошти, месенджерів у робочі дні

## 2. Анотація дисципліни

Курс «Безпека баз даних» спрямований на формування теоретичних знань і практичних навичок забезпечення конфіденційності, цілісності та доступності даних у сучасних інформаційних системах. У межах курсу розглядаються основні моделі загроз для СУБД, механізми контролю доступу, аудиту та журналювання, криптографічні методи захисту, а також типові вразливості під час роботи з SQL-запитами та прикладними сервісами, що використовують бази даних. Під час навчання студенти знайомляться з практиками налаштування захищеної конфігурації СУБД (наприклад, PostgreSQL/MySQL), керування ролями та привілеями, організації резервного копіювання, відновлення і реплікації..

## 3. Мета і завдання дисципліни

**Метою викладання дисципліни** «Безпека баз даних» є формування у здобувачів вищої освіти системних знань про сучасні підходи, методи й інструменти захисту баз даних та розвиток практичних умінь щодо впровадження політик доступу, налаштування захищеного середовища СУБД і протидії типовим атакам на дані в корпоративних інформаційних системах.

Основними **завданнями** вивчення дисципліни є ознайомлення здобувачів вищої освіти з основними загрозами та моделями атак на бази даних; формування навичок організації контролю доступу до даних на основі ролей, привілеїв і політик безпеки; опанування методів захищеної конфігурації та адміністрування СУБД у середовищі корпоративних інформаційних систем; набуття практичних умінь застосування засобів аудиту, журналювання та моніторингу подій безпеки; вивчення криптографічних механізмів захисту даних (шифрування, хешування, керування ключами) та організації резервного копіювання і відновлення; розвиток компетентностей із протидії типовим вразливостям прикладного рівня (зокрема SQL-ін'єкціям) і побудови безпечної взаємодії прикладних сервісів із базами даних.

## 4. Результати навчання

У результаті вивчення дисципліни здобувач вищої освіти повинен:

- Виявляти основні загрози безпеці баз даних, аналізувати вразливості СУБД та оцінювати можливі наслідки інцидентів;
- Налаштовувати механізми автентифікації, авторизації та розмежування доступу до даних відповідно до визначених політик безпеки;
- Реалізовувати комплекс заходів захисту даних у СУБД (аудит, журналювання, резервне копіювання, відновлення, контроль цілісності);

– Застосовувати практичні методи захисту від типових атак на бази даних (зокрема SQL-ін'єкцій), а також використовувати криптографічні засоби для забезпечення конфіденційності інформації.

## 5. Обсяг дисципліни

Ознака дисципліни	
Кількість кредитів / годин	4/120
Нормативна / вибіркова	вибіркова
Вид підсумкового контролю	залік

## 6. Політика дисципліни

### Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення. Детальніше за посиланням URL : <http://www.kntu.kr.ua/doc/dobro.pdf>

### Відвідування занять

Відвідування занять є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і лабораторні заняття курсу.

Пропущені заняття повинні бути відпрацьовані не пізніше, ніж за тиждень до залікової сесії.

### Поведінка на заняттях

**Недопустимість:** запізнь на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

При організації освітнього процесу в Центральноукраїнському національному технічному університеті студенти, викладачі та адміністрація діють відповідно до: Положення про організацію освітнього процесу; Положення про організацію вивчення навчальних дисциплін вільного вибору; Положення про рубіжний контроль успішності і сесійну атестацію студентів ЦНТУ, Кодексу академічної доброчесності ЦНТУ.

## 7. Програма навчальної дисципліни

### **Тема 1. Вступ до безпеки баз даних**

Поняття безпеки БД, моделі порушника та загроз.

Типові ризики витоку, модифікації та втрати даних.

### **Тема 2. Політика доступу та управління правами в СУБД**

Ролі, привілеї, принцип мінімальних повноважень.

Моделі керування доступом (DAC, MAC, RBAC).

### **Тема 3. Автентифікація та авторизація користувачів БД**

Методи автентифікації (паролі, токени, MFA).

Централізована автентифікація (LDAP/AD), керування сесіями.

**Тема 4. Захист від атак на бази даних**

SQL-ін'єкції, XSS у зв'язці з БД, brute-force, privilege escalation.

Методи запобігання та практики secure coding.

**Тема 5. Журналювання та аудит подій у базах даних**

Аудит доступу, журнал операцій, контроль змін.

Виявлення підозрілої активності та аналіз логів.

**Тема 6. Криптографічний захист даних у СУБД**

Шифрування даних «на диску» та «в каналі».

Хешування паролів, керування ключами, TLS.

**Тема 7. Резервне копіювання та відновлення. Забезпечення доступності**

Стратегії backup/restore, RPO/RTO.

Реплікація, кластеризація, відмовостійкість.

**Тема 8. Комплексний захист БД у корпоративній інфраструктурі**

Безпечне налаштування СУБД (hardening).

Контроль конфігурацій, оновлення, моніторинг і реагування на інциденти.

## 8. Система оцінювання та вимоги

**Види контролю:** поточний, підсумковий.

**Методи контролю:** спостереження за навчальною діяльністю, усне опитування, письмовий контроль, тестовий контроль.

**Форма підсумкового контролю:** залік.

Поточний контроль у межах дисципліни здійснюється через оцінювання виконання кожної лабораторної роботи. Під час виставлення балів враховуються коректність розв'язання поставленого завдання, рівень підготовки та аргументованість захисту результатів, а також дотримання визначених строків виконання. Додатково оцінюється ступінь засвоєння теоретичних положень і сформованість практичних умінь.

Підсумковий контроль проводиться у формі заліку та спрямований на перевірку рівня опанування навчального матеріалу і здатності здобувача застосовувати знання під час виконання практичних завдань.

## 9. Рекомендована література

### Базова

1. Silberschatz A., Korth H.F., Sudarshan S. Database System Concepts. 7th Edition. – New York: McGraw-Hill Education, 2019. – 1376 p.
2. Elmasri R., Navathe S.B. Fundamentals of Database Systems. 7th Edition. – Boston: Pearson, 2016. – 1248 p.
3. Kleppmann M. Designing Data-Intensive Applications: The Big Ideas Behind Reliable, Scalable, and Maintainable Systems. – Sebastopol: O'Reilly Media, 2017. – 616 p.
4. Harrison G., Lane K., Paul D. Database Modeling and Design: Logical Design. 5th Edition. – Burlington: Morgan Kaufmann, 2015. – 560 p.
5. Stallings W., Brown L. Computer Security: Principles and Practice. 5th Edition. – Boston: Pearson, 2018. – 840 p.

6. Whitman M.E., Mattord H.J. Principles of Information Security. 7th Edition. – Boston: Cengage Learning, 2021. – 720 p.
7. Halfond W.G.J., Viegas J., Orso A. SQL Injection Attacks and Defense. 2nd Edition. – Burlington: Syngress (Elsevier), 2012. – 592 p.

#### **Допоміжна**

8. Madhavan R. (ed.) Database Security and Auditing: Protecting Data Integrity and Accessibility. – Burlington: Elsevier/Morgan Kaufmann, 2014. – 368 p.
9. Shema M. MongoDB Security. – Birmingham: Packt Publishing, 2015. – 244 p.
10. Niemiec R. Oracle Database 12c Performance Tuning Recipes. – New York: Apress, 2014. – 480 p. (корисно для розділів “захист + продуктивність, аудит, контроль доступу”)

#### **Інформаційні ресурси**

11. Онлайн-курси Prometheus. – URL: <https://prometheus.org.ua/>
12. Онлайн-курси Coursera. – URL: <https://www.coursera.org>
13. Академія Cisco. – URL: <https://www.netacad.com>
14. Он-лайн ресурс з інформаційних технологій. – URL: <https://dou.ua/>
15. Пошукова система. – URL: <https://www.google.com/>
16. Он-лайн ресурс перегляду відеоуроків.– URL: <https://www.youtube.com>