

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ РАДІО, ТЕЛЕБАЧЕННЯ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Галузь знань:
**12 – Інформаційні
технології**

Спеціальність:
125 – Кібербезпека

Підготовка:

Ведеться за програмою, що передбачає здачу іспиту та отримання сертифікату **CISSP** наприкінці 4-го курсу, одночасно з дипломом бакалавра з кібербезпеки



Сертифікат CISSP (Certified Information Systems Security Professional, Сертифікований спеціаліст з безпеки інформаційних систем) є глобально визнаним стандартом з кібербезпеки. CISSP передбачає всебічну, актуальну, глобальну загальну сукупність знань, що гарантує, щоб у спеціалістів з кібербезпеки були глибокі знання й розуміння нових загроз, технологій, інструкцій, стандартів і методів.

Іспит CISSP перевіряє компетентність в 8 областях:

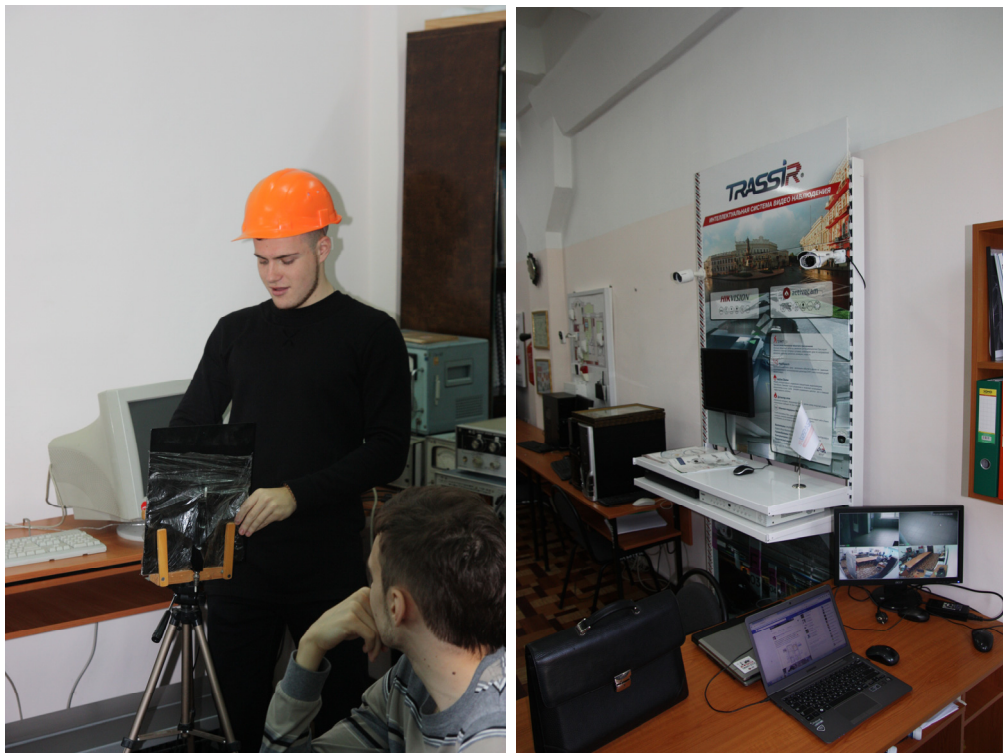
- 1) безпека і керування ризиками;
- 2) безпека активів;
- 3) інженерія безпеки;
- 4) безпека комунікацій і мереж;
- 5) керування ідентифікацією й доступом;
- 6) оцінки безпеки і тестування;
- 7) операції із забезпечення безпеки;
- 8) безпека розробки програмного забезпечення.

Власники сертифікату CISSP мають можливість **працювати у будь-якій країні**, де потрібні професіонали з кібербезпеки. Наприклад, на посадах:

- Консультант із систем безпеки
- Директор/менеджер ІТ
- Архітектор систем безпеки
- Інженер систем безпеки
- Директор підрозділу інформаційної безпеки
- Менеджер з безпеки
- Аудитор з безпеки
- Аналітик з питань безпеки
- Архітектор комп'ютерних мереж

Детальна інформація про сертифікат CISSP та відповідну програму навчання <https://www.isc2.org/cissp/default.aspx>.

На 1-2 курсах навчання передбачається інтенсивне вивчення англійської мови (щоденні заняття), з метою отримання студентами після 2-го курсу сертифікату B2. Вільне володіння англійською мовою та знання англійської термінології з кібербезпеки необхідно для успішної праці в цій галузі незалежно від країни, де працює спеціаліст.



Випускники за спеціальністю Кібербезпека також навчаються кваліфіковано здійснювати проектування, розроблення, експлуатацію, модернізацію та технічне обслуговування засобів захисту інформації; організувати функціонування комплексних систем захисту інформації; виконувати аналітико-теоретичні дослідження в галузі кібербезпеки; проектувати, створювати та експлуатувати системи банківської безпеки; тестувати та вдосконалювати власні і сторонні розробки для уникнення ризиків витоку інформації; організувати захист інформації в інфокомунікаційних системах і мережах та глобальній мережі Інтернет.

Тел. ННІ РТ та ІБ (048) 705-02-93 з 9.00 до 16.00