Анотація навчальної дисципліни вільного вибору здобувача вищої освіти

Дисципліна:	**«Основи кібербезпеки»**
Викладач:	**Крет Роман Михайлович, к.політ.н., доцент**
E-mail:	Roman.kret@rshu.edu.ua
Кількість кредитів:	**3**
Мова викладання:	**українська**
Вид контролю:	**залік**
Місце у структурно-логічній схемі:	**вивчається в 8 семестрі першого (бакалаврського) рівня вищої освіти за спеціальностями:** **113 Прикладна математика** **121 Іженерія програмного забезпечення** **122 Комп'ютерні науки**

Вступ

На сучасному етапі Інтернет значно впливає на наш спосіб життя, включаючи робочі процеси, навчання чи розваги. Останнім часом до Інтернету можуть бути підключені не тільки комп'ютери, а й всілякі інші «девайси», оснащені сенсорами, датчиками і пристроями передачі інформації, які людина може використовувати в повсякденному житті.

Проте поряд з перевагами сучасного цифрового світу і розвитком інформаційних технологій, в цей час активно поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконних фінансових операцій, крадіжок і шахрайства в мережі Інтернет. Сучасні інформаційно-комунікаційні технології активно використовуються як у мирний час, так і під час військових дій.

Кібербезпека – дуже важливий аспект освіти сучасного студента. Кожен здобувач освіти повинен володіти навичками грамотного поводження з інформацією. Кіберзагрози існують повсюди де застосовуються інформаційні технології, отже, студент будь-якої спеціальності, враховуючи умови сьогодення, в своїй діяльності стикається і зі спамом, і з вірусами, і зі зломом комп'ютера і з багатьма іншими проблемами, на які потрібно вміти оперативно реагувати, а ще краще, запобігти.

Предмет «Основи кібербезпеки» належить до вибіркових дисциплін циклу професійної підготовки бакалаврів спеціальностей 113 Прикладна математика, 121 Інженерія програмного забезпечення, 122 Комп'ютерні науки. Для майбутніх фахівців цих спеціальностей важливе оволодіння необхідними базовими поняттями та правилами безпечної поведінки в мережі, ознайомлення з різними типами зловмисного програмного забезпечення та атаками, а також методами захисту від них.

Передумови для вивчення дисципліни: Базові знання інформатики та комп'ютерної техніки.

Мета та завдання дисципліни

Метою вивчення дисципліни є ознайомлення здобувачів вищої освіти спеціальностей 113 «Прикладна математика», 121 «Інженерія програмного забезпечення», 122 «Комп'ютерні науки» із методами та підходами до забезпечення безпечного та продуктивного ІТ-середовища в аспекті інформатизації та діджиталізації громад.

Основними **завданнями** вивчення дисципліни «Основи кібербезпеки» є навчитись безпечно поводитись в Інтернеті: користуватися обліковими записами, використовувати програмні додатки захисту, шифрування та кодування інформації, опанувати основні правила інформаційної гігієни.

Очікувані результати навчання

У результаті вивчення дисципліни «Основи кібербезпеки» студенти повинні
знати:

- основні аспекти кібергігієни та організації безпечної взаємодії з інформаційними системами та сервісами;
- різновиди шкідливого програмного забезпечення та методи протидії кіберзагрозам;
- методи і засоби безпечної авторизації, забезпечення безпечного зберігання та доступу до даних;
- основи безпеки комп'ютерних мереж, бездротових з'єднань, IoT;
- методи і засоби безпечного віддаленого доступу до інформаційних ресурсів та сервісів;
- безпека мобільних пристроїв;
- основи безпечного користування соціальними мережами, Internet-месенджерами, web-ресурсами.

вміти:

- здійснювати аналіз та визначення можливих загроз в процесі користування інформаційними сервісами та ресурсами;
- використовувати методи, засоби попередження та протидії кіберзагрозам;
- організовувати безпечне локальне та віддалене зберігання, оперування даними;
- використовувати цифровий підпис;
- організовувати безпечний та комфортний власний інформаційний простір в сучасному цифровому світі.

Програма навчальної дисципліни

«Безпечний доступ до сервісів державної і місцевої влади»:

- Огляд державних сервісів та інструментів взаємодії з ними
- Комплекс заходів щодо безпечного доступу до державних сервісів
- Вразливості QR-кодів та сценарії безпечного користування
- Безпека парольного доступу
- Двофакторна (двоетапна) авторизація
- Доступ з використанням апаратних ключів
- Доступ з використанням електронного цифрового підпису

«Безпека персональних даних в розрізі діджиталізації»:

- Е-профіль громадянина в сучасному ІТ світі
- Джерела персональних даних в ІТ середовищі. Довірені та недовірені засоби
- Онлайн серфінг
- Пошукові сервіси
- Електронна пошта
- Додатки та електронні книги
- Соціальні мережі
- Телефон
- Транспорт
- Покупки
- Камери спостереження
- Водіння транспорту
- Кредитно-інформаційні служби

- Державні реєстри
- Ознаки порушення приватності персональних даних при е-взаємодії та сценарії протидії
- Інформація про особу та персональні дані
- Персональні дані та конфіденційна інформація

«Безпека взаємодії державних установ при наданні електронних послуг»:

- Безпека отримання е-послуг offline, через центри надання адміністративних послуг
- Безпека отримання е-послуг online, через віддалене підключення