

- введенні модульно-рейтингових систем вивчення нормативних курсів, що надає можливість реального поєднання процесу викладання та самостійної роботи студентів;

- наявності пакетів нормативних джерел, що використовуються студентами в процесі підготовки до семінарських та практичних занять з нормативних дисциплін, які формують майбутнього спеціаліста.

Засвоєння дисциплін повинно відбуватися в контексті майбутньої діяльності за трьома базовими типами навчальної роботи:

- академічним (з провідною роллю лекцій і семінарів);
- квазіпрофесійним (з широким використанням ігрових занять);
- навчально-професійним (виробнича практика, написання курсових і дипломних робіт), який є важливим стимулом інтенсифікації навчання студентів.

Професійна спрямованість орієнтує студента на такі цінності, як сумлінне засвоєння майбутньої спеціальності, оволодіння професійною майстерністю, створення нових, більш ефективних алгоритмів діяльності.

Таким чином, використання нових інтенсивних технологій навчання розвиває творчі здібності і нахили студентів, формує у них культуру мислення, уміння самостійно орієнтуватися в суспільно-політичній, економічній і науковій інформації.

Н.В. Баловсяк, канд. пед. наук, доцент,
balovsyak@mail.ru

Чернівецький торговельно-економічний інститут КНТЕУ, м. Чернівці

ЗАХИСТ ОСОБИСТИХ ДАНИХ ЯК ЕЛЕМЕНТ ЗМІСТУ ОСВІТИ ПРИ ВИВЧЕННІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Вивчення інформаційних технологій як елемент підготовки сучасного фахівця повинно враховувати зміни в суспільстві, структурі та змісті професійної діяльності та веденні бізнесу. На сьогодні Інтернет є невід'ємною складовою частиною життя і професійної діяльності сучасних спеціалістів. Тому тенденції розвитку сучасної мережі Інтернет відповідним чином повинні бути відображені у змісті освіти при вивченні інформаційних технологій.

Основним напрямком розвитку Інтернету в останні два роки є виникнення цілого ряду так званих соціальних сервісів, які базуються на основі UGC (user generated content). Суть такого типу сервісів полягає в тому, що користувачі, тобто відвідувачі їх сайтів є не лише споживачами, а й авторами контенту. Тобто користувачі створюють

зміст сайту, який потім стає доступним для інших користувачів Інтернету.

Популярність соціальних сервісів призвела до появи нової проблеми, яка не була відома і актуальна до недавнього часу – це онлайн-приватність.

Приватність виражається як у захисті користувача від стороннього доступу, так і в захисті його дій, що починаються в Інтернеті, як щодо стороннього доступу, так і використання цих даних проти користувача. Ця проблема особливо актуальна в наш час. З іншого боку – онлайн зводить нанівець усіляку приватність. Однак знаючи про цю проблему, можна себе відгородити від можливого порушення цієї приватності. Не дивлячись на те, що більшість онлайн-сервісів підтримують можливість налаштування прав доступу таким чином, щоб сторонні користувачі не могли переглядати дані, розміщені на сайті користувачами, більшість цими елементарними правилами безпеки нехтують, а також часто використовують свої точні контактні дані, правильні імена, номери мобільних телефонів тощо.

Таким чином, сучасний фахівець повинен володіти знаннями про забезпечення особистої приватності і навичками захисту особистих даних при роботі в Інтернеті.

Для цього у зміст дисциплін, предметом вивчення яких є інформаційні технології, повинні бути включені ряд питань, присвячених основам онлайн-безпеки та забезпеченню приватності роботи в Інтернеті. Якщо в структурі підготовки користувачів з інформаційних технологій не передбачено окремого курсу, присвяченого інформаційній безпеці та захисту інформації, то розділи, присвячені мережевій безпеці та онлайн-приватності повинні бути включені в загальні дисципліни. Відповідні лабораторні та практичні заняття повинні містити завдання, згідно з якими студенти б розглянули базові елементи пошуку в Інтернеті, окрім цього – налаштування соціальних сервісів щодо обмеження доступу до особистих даних користувача інших осіб.

Поряд з цим не слід забувати про елементарні правила організації безпечної роботи в Інтернеті, які досягаються, в тому числі, використанням такого базового програмного забезпечення як антивірусні програми, мережеві екрани (файрволи), програми для видалення Spyware.