МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ НАВЧАЛЬНИЙ ЗАКЛАД
“ВИЩЕ ПРОФЕСІЙНЕ УЧИЛИЩЕ № 34 м. СТРИЙ”

ЗАТВЕРДЖУЮ
заступник директора
з навчально-виробничої роботи
ДНЗ “ВПУ-34 м. Стрий”
_____ Леся ПАВЛІВ
.

РОБОЧА ПРОГРАМА
з навчальної дисципліни “Основи кібергігієни”
за освітньо-професійним ступенем фаховий молодший бакалавр

Спеціальність: **182 Технології легкої промисловості**

Галузь знань: **18 Виробництво та технології**

Розглянуто та схвалено на засіданні циклової комісії
Протокол №___від”____” _____2023р.
Голова циклової комісії _____Леся СЕНЦОВА

Розробив викладач _____Ігор ЯРИЧ

МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна дисципліна “Основи кібергігієни” є вибірковою для підготовки спеціалістів широкого профілю із загально-технічних спеціальностей.

Програму розраховано на студентів, які навчаються за освітньо-кваліфікаційним рівнем “фаховий молодший бакалавр” технічного спрямування.

Згідно з навчальним планом на вивчення дисципліни “Основи кібергігієни” виділено всього 23 академічних години (0,77 кредиту ECTS).

Вивчення дисципліни базується на знаннях, отриманих при вивченні предметів “Інформатика”, “Інформаційні технології” та вміннях працювати на персональному комп’ютері в обсязі, достатньому для виконання професійних обов’язків.

Предметом навчальної дисципліни “Основи кібергігієни” є методи, способи та профілактичні заходи, які потрібно застосовувати в повсякденному житті для захисту від цифрових загроз, таких як зловмисне програмне забезпечення, програми-вимагачі, фішинг, крадіжка особистих фінансів та особистих даних, а також кібербулінг.

Метою викладання навчальної дисципліни “Основи кібергігієни” є формування базових знань механізму безпеки під час роботи за комп’ютером, що стосуються кібергігієни на робочу місці, вивчення нормативно-правової бази у сфері кібергігієни та інформаційної безпеки, здійснення заходів з кібергігієни на робочому місці та ефективне використання сучасних комп'ютерно-інформаційних технологій у своїй діяльності, що має забезпечити формування у здобувачів освіти основ інформаційної культури та інформаційно-комунікативної компетентності та набуття практичних навичок щодо їх застосування у майбутній професії.

Завдання дисципліни “Основи кібергігієни” полягає у наступному:

- ✓ вмінні ідентифікувати кіберзагрози для пересічних користувачів;
- ✓ вмінні ідентифікувати ознаки атак на пересічних користувачів та реагувати на них, забезпечуючи власну цифрову безпеку;
- ✓ вмінні ідентифікувати кібербулінг та протистояти його проявам;
- ✓ визначати заходи кібергігієни для конкретної ситуації;
- ✓ оцінювати загрози та вживання заходів реагування на робочому місці;
- ✓ безпечно поводитись у кіберсфері;
- ✓ здійснювати організацію безпечного доступу до пристроїв і програм;
- ✓ правильно налаштовувати програмне забезпечення на робочому місці;
- ✓ вмінні здійснювати оцінювання інформації згідно принципів онлайн-конфіденційності та цифрового сліду.

Очікувані результати вивчення дисципліни “Основи кібергігієни”:

1. кваліфіковане та ефективне використання сучасних інформаційно-комунікаційних технологій у навчально-пізнавальній діяльності та повсякденному житті;
2. уміння самостійно опановувати та раціонально використовувати програмні засоби різного призначення, цілеспрямовано шукати й систематизувати інформацію, використовувати електронні засоби обміну даними;
3. уміння застосовувати інформаційно-комунікаційні технології з метою ефективного розв’язання різноманітних завдань щодо отримання, обробки, збереження, подання інформації, які пов’язані з майбутньою професійною діяльністю в умовах інформаційного суспільства.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Вступний інструктаж з правил техніки безпеки.
Тема 1. Вступ до кібергігієни та протидії кібербулінгу. Важливість людського фактору у системі безпеки. Види хакерських атак. Визначення поняття “кібергігієна”.
Тема 2. Соціальна інженерія. Поняття соціальної інженерії. Причини та умови соціальної інженерії. Прийоми, методи та принципи соціальної інженерії. Психологія впливу та загальні рекомендації для здобувачів освіти.
Тема 3. Безпечне користування мережею Інтернет. Браузер та його функції. Доменні імена. Шифрування комунікацій. Організація авторизації в Інтернеті з використанням браузера. Безпечне використання плагінів. Рекомендації з убезпечення браузера. Безпечне користування мережами Wi-Fi. Відповідальне оприлюднення інформації.
Тема 4. Безпечне користування електронною поштою. Розмежування використання особистої та службової поштових скриньок. Загрози під час користування поштовою скринькою. Аналіз листів, що містять ознаки фішингу. Рекомендації щодо захисту електронної пошти. План дій на випадок компрометації пошти.
Тема 5. Шкідливе програмне забезпечення. Загрози для програмного забезпечення. Оновлення програмного забезпечення. Ліцензійне та неліцензійне програмне забезпечення. Типи шкідливого програмного забезпечення. Загальні рекомендації з використання програмного забезпечення. Антивіруси: міфи та реалії.
Тема 6. Безпека користування соціальними мережами. Соціальні мережі: загальні положення. Безпечна реєстрація в соціальних мережах. Налаштування конфіденційності та інших питань безпеки. Шахрайство в соціальних мережах. Відповідальне поширення інформації у соціальних мережах. Рекомендації з безпечної роботи в соціальних мережах.
Тема 7. Безпека мобільних пристроїв. Правила обмеження доступу до мобільних пристроїв. Особливості передавання контактної інформації іншим особам. Головні загрози, які виникають під час роботи з мобільними пристроями. Основні правила безпечної роботи з мобільними пристроями.
Тема 8. Фізична безпека. Роль фізичної безпеки у кіберзахисті. Безпека контрольованої зони. Загрози, які виникають під час використання змінних носіїв інформації. Зв’язок соціальної інженерії та фізичної безпеки.
Тема 9. Убезпечення від неправдивих повідомлень. Види маніпуляцій з інформацією у кіберсфері. Розпізнавання фейків в Інтернеті. Заходи протидії неправдивим повідомленням.
Тема 10. Протидія кібербулінгу. Кібербулінг – як розпізнати? Тролінг та флеймінг. Наклепи та переслідування (сталкінг). Гепіслепінг. Секстинг та онлайн-грумінг. Шпигунство та самозванство.
Тема 11. Правові засади кібергігієни. Правові засади кібергігієни в законодавстві України.
Підведення підсумків вивченого. Комп’ютерне тестування

ТЕМАТИЧНИЙ ПЛАН ДИСЦИПЛІНИ

Тема заняття	Кількість годин
Вступний інструктаж з правил техніки безпеки. Тема 1. Вступ до кібергігієни та протидії кібербулінгу	**2**
Тема 2. Соціальна інженерія	**2**
Тема 3. Безпечне користування мережею Інтернет	**2**
Тема 4. Безпечне користування електронною поштою	**2**
Тема 5. Шкідливе програмне забезпечення	**2**
Тема 6. Безпека користування соціальними мережами	**2**
Тема 7. Безпека мобільних пристроїв	**2**
Тема 8. Фізична безпека	**2**
Тема 9. Убезпечення від неправдивих повідомлень	**2**
Тема 10. Протидія кібербулінгу	**2**
Тема 11. Правові засади кібергігієни	**2**
Підведення підсумків вивченого. Комп'ютерне тестування	**1**
Разом	**23**

МЕТОДИ НАВЧАННЯ ТА КОНТРОЛЮ, КРИТЕРІЇ ОЦІНЮВАННЯ, РЕКОМЕНДОВАНА ЛІТЕРАТУРА

При проведенні лекцій використовуються **словесні та наочні методи**:

- ✓ пояснення з елементами бесіди;
- ✓ демонстрація за допомогою ПК.

Методи контролю:

- ✓ усний контроль;
- ✓ комбінований контроль;
- ✓ підсумковий контроль.

При оцінювані відповіді студента потрібно керуватися такими **критеріями**:

- ✓ повнота і правильність відповіді;
- ✓ ступінь усвідомлення і розуміння вивченого;
- ✓ мовне оформлення відповіді.

Відповідь студента має бути зв'язаною, логічною, послідовною.

Оцінювання якості підготовки студентів з навчальної дисципліни "Основи кібергігієни" здійснюється в двох аспектах:

- ✓ рівень володіння теоретичними знаннями;
- ✓ здатність до застосування вивченого матеріалу у практичній діяльності.

Критерії оцінювання знань учнів

Оцінка „відмінно» (високий рівень). Студент володіє узагальненими знаннями навчального матеріалу в повному. Відповідь студента повна, правильна, логічна і містить аналіз, систематизацію, узагальнення навчального матеріалу. Студент вміє самостійно знаходити і користуватися джерелами інформації, оцінювати отриману інформацію. Встановлює причинно-наслідкові та міжпредметні зв'язки. Робить аргументовані висновки. Правильно і усвідомлено застосовує всі види довідкової інформації в межах на5альної програми. Проявляє пізнавально-творчий інтерес до обраної професії.

Оцінка „добре» (достатній рівень). Студент самостійно, з розумінням відтворює основний навчальний матеріал та застосовує його при виконанні завдань в типових умовах (стандартних ситуаціях). Дає визначення основних понять, аналізує, порівнює інформацію, встановлює її зв'язок з обраною професією та робить висновки. Відповідь в цілому правильна, логічна та достатньо обґрунтована. При відповіді допускає несуттєві помилки, які може виправити.

Оцінка „задовільно» (задовільний рівень). Студент на рівні запам'ятовування, без достатнього розуміння, відтворює основні положення навчального матеріалу. Дає помилкові визначення основних понять. Може частково обґрунтувати і проаналізувати свою відповідь. При відповіді допускає помилки, які самостійно не може виправити.

Оцінка „незадовільно» (незадовільний рівень). Студент, за допомогою викладача відтворює на рівні розпізнавання окремі фрагменти навчального матеріалу. При відповіді допускає суттєві помилки.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Кібергігієна та протидія кібербулінгу. Посібник для проведення навчань молоддю для молоді, розроблений в межах програми «Мріємо та діємо», 2022.
2. Манжай О., Носов В. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікатної) програми підвищення кваліфікації: Практикум. – К.: ВАІТЕ, 2021.