ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра журналістики та реклами

ЗАТВЕРДЖЕНО
вченою радою
(пост. п. 9 від «30» 06 2022 р.)
Ректор
_____ А. А. Мазаракі

ОСНОВИ КІБЕРБЕЗПЕКИ /
CYBERSECURITY ESSENTIALS

ПРОГРАМА /
COURSE SUMMARY

Київ 2022

Автори: Ю.В. КОСТЮК, старший викладач кафедри інженерії програмного забезпечення та кібербезпеки,
Т.В. САВЧЕНКО кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
Л.О. ВЛАСЕНКО, кандидат технічних наук, доцент, кафедри інженерії програмного забезпечення та кібербезпеки

Програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки «14» травня 2022р., протокол №38.

Рецензенти: Н.О. Котенко, кандидат педагогічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
В.П. Звєрєв, кандидат технічних наук, заступник керівника служби з питань інформаційної безпеки та кібербезпеки – керівник управління інформаційної безпеки Апарату Ради Національної безпеки і оборони України,
І.М. Овдієнко, кандидат психологічних наук, доцент кафедри психології

ОСНОВИ КІБЕРБЕЗПЕКИ /
CYBERSECURITY ESSENTIALS

ПРОГРАМА /
COURSE SUMMARY

ВСТУП

Дисципліна «Основи кібербезпеки» є вибірковою компонентою навчального плану підготовки студентів денної форми навчання першого (бакалаврського) рівня вищої освіти за спеціальністю 053 «Психологія», галузі знань 05 «Соціальні та поведінкові науки», освітня програма «Практична психологія».

Програму підготовлено відповідно до Стандарту вищої освіти України із зазначеної спеціальності та відповідної освітньо-професійної програми підготовки бакалаврів ДТЕУ.

Програма складається з таких частин:

1. Мета, завдання та предмет дисципліни.
2. Передумови вивчення дисципліни як вибіркової компоненти освітньої програми.
3. Результати вивчення дисципліни.
4. Зміст дисципліни.
5. Список рекомендованих джерел.

1. МЕТА, ЗАВДАННЯ ТА ПРЕДМЕТ ДИСЦИПЛІНИ

Метою дисципліни «Основи кібербезпеки» є формування у майбутніх фахівців необхідного рівня знань щодо правильного поводження з інформацією у кіберсфері та безпечної роботи із засобами комп'ютерної техніки в професійній діяльності; дізнатись про основні загрози в сучасному інформаційному просторі; аналізувати поширені помилки користувачів та наслідки від атак зловмисників і кібершахраїв; вивчити базові правила захисту інформації на персональних електронних пристроях та в соціальних мережах; навчитись визначати фейкові новини; опанувати основні рекомендації щодо захисту власних даних, безпечного користування електронними пристроями та інформаційними ресурсами.

Завданнями вивчення дисципліни «Основи кібербезпеки» є засвоєння студентами:

- ✓ знання основних положень, термінів та заходів, що стосуються кібергігієни на робочу місці;
- ✓ знання основної нормативно-правової бази у сфері кібербезпеки та інформаційної безпеки;
- ✓ знання особливостей кібергігієни в системі публічної служби.
- ✓ уміння визначати заходи кібергігієни для конкретної ситуації;
- ✓ уміння оцінювати загрози та вживати заходів реагування на

робочому місці;

- ✓ уміння безпечно поводитись у кіберсфері.
- ✓ навички організації безпечного доступу до пристроїв і програм;
- ✓ навички правильного налаштування програмного забезпечення на робочому місці;
- ✓ навички критичного оцінювання інформації;
- ✓ знати різні типи зловмисного ПЗ (відомого як шкідливі програми) та їх симптоми; знати різні методи, якими нападники можуть проникнути в систему: соціальна інженерія, злам паролю Wi-Fi, фішинг та використання вразливостей, тощо.

Предметом дисципліни «Основи кібербезпеки» є інформаційні технології, комп'ютерне устаткування.

2. ПЕРЕДУМОВИ ВИВЧЕННЯ ДИСЦИПЛІНИ ЯК ВИБІРКОВОЇ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

знання:

- інформаційних технологій в професійній діяльності;
- іноземної мови за професійним спрямуванням;

вміння: вільно працювати:

- з офісними додатками Microsoft;
- з хмарними сервісами Office 365;
- з пошуковою системою Google;

3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Дисципліна «Основи кібербезпеки», як вибіркова компонента освітньої програми, забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за відповідною освітньо-професійною програмою:

«Практична психологія» (ОС бакалавр)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності		

ЗК3	Навички використання інформаційних і комунікаційних технологій	1-14
ЗК4	Здатність вчитися і оволодівати сучасними знаннями	7 8, 9, 12, 13, 14
ЗК10	Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні	1, 3, 5, 6, 12
Спеціальні (фахові, предметні) компетентності		
СК3	Здатність до розуміння природи поведінки, діяльності та вчинків	3, 6, 9, 12
СК10	Здатність дотримуватися норм професійної етики	13, 14
Програмні результати навчання за освітньою програмою		
ПР3	Здійснювати пошук інформації з різних джерел, у т.ч. з використанням інформаційно-комунікаційних технологій, для вирішення професійних завдань	1-14
ПР13	Взаємодіяти, вступати у комунікацію, бути зрозумілим, толерантно ставитися до осіб, що мають інші культуральні чи гендерно-вікові відмінності	9

4. ЗМІСТ ДИСЦИПЛІНИ

Тема 1. Кіберпростір і кібербезпека — головні ознаки нової інформаційної цивілізації

Поняття інформаційна безпека, кібербезпека, кіберпростір, кіберборотьба, кібертероризм, кіберзброя. Кіберпростір як сфера ведення війн сучасності та майбутнього. Сутність кібербезпеки інформаційного суспільства. Кіберінциденти: передумови скоєння та наслідки.

Дії у кіберпросторі та їх особливості. Класифікація форм і способів кібердій. Основи кіберрозвідки. Основи кіберзахисту.

Огляд областей кібербезпеки. Приклади доменів кібербезпеки. Зростання кібер-доменів. Поняття «кіберзлочинець» та мотиви кіберзлочинів. Класифікація зловмисників.

Список рекомендованих джерел:

Основний: 1[с. 50-59, 66-98, 257-268, 310-312], 2 [с. 7-43], 3 [с. 27-38, 130-146], 4 [с. 112-120].

Додатковий: 6 [с. 25-28, 172-176, 239, 249-252, 255-263].

Інтернет-ресурси: 14.

Тема 2. Національна система кібербезпеки України

Основні положення Стратегії кібербезпеки України. Сутність та завдання Національної системи забезпечення кібербезпеки України Пріоритети та напрями забезпечення кібербезпеки України згідно з чинним законодавством. Захист відкритої інформації в державних органах. Компетенція органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці.

Правове забезпечення у сфері інформаційної безпеки та кібербезпеки. Структура національної безпеки України. Суб'єкти забезпечення інформаційної безпеки як складової національної безпеки України. Основні пріоритети забезпечення інформаційної безпеки.

Список рекомендованих джерел:

Основний: 1 [с. 135-149], 2 [с. 7-24], 3 [с. 222-240], 4 [с. 137-138].

Додатковий: 6 [с. 189-209], 7 [с. 93-106], 10, 11, 12.

Інтернет-ресурси: 14, 16.

Тема 3. Сутність та основні процедури керування кібербезпекою

Модель кібербезпеки ISO. Огляд моделі. Галузі кібербезпеки. Цілі контролю. Контроль. Використання моделі ISO для кібербезпеки. Модель кібербезпеки ISO та тріада КЦД. Модель кібербезпеки ISO і можливі стани даних. Модель кібербезпеки ISO і технології захисту.

Список рекомендованих джерел:

Основний: 1 [с. 54-59], 3 [с. 157-166].

Додатковий: 6 [с. 218-219].

Інтернет-ресурси: 14, 15, 16.

Тема 4. Кібератаки, загрози та їх властивості. Характеристика сучасних кібератак

Комп'ютерні атаки та технології їхнього виявлення. Сутність та класифікація кібератак. Етапи реалізації атак.

Відмова в обслуговуванні. Аналіз трафіку (Sniffing). Підміна. Man-in-the-middle. Атаки нульового дня. Клавіатурні шпигуни (кейлогери). Захист від атак.

Атаки на бездротові мережі та мобільні пристрої. Grayware та SMiShing. Несанкціоновані точки доступу. Глушіння радіочастот (RF Jamming). Bluejacking та Bluesnarfing. Атаки на WEP та WPA. Захист від атак на бездротові мережі та мобільні пристрої.

Атаки на застосунки. Міжсайтовий скриптинг. Ін'єкція коду. Переповнення буфера. Віддалений запуск програм. Захист від атак на застосунки.

Атака "Відмова в обслуговуванні" (DoS). Розподілена DoS атака (Distributed DoS Attack, DDoS). Отруєння SEO.

Зміст, класифікація та ознаки кіберзагроз. Основні характеристики кіберзагроз. Внутрішні та зовнішні кіберзагрози. Кіберзагрози через Інтернет-сервіси. Поширення кіберзагроз. Кіберзагрози підвищеної складності.

Список рекомендованих джерел:

Основний: 1 [с. 66-96, 168-179], 2 [с. 43-62], 3 [с. 92-138], 4 [с. 9-23].

Додатковий: 6 [с. 296-299, 340-354], 8 [с. 50-82, 197-201].

Інтернет-ресурси: 14, 15.

Тема 5. Дезінформація як елемент кібератак. Сценарії розвитку та методи протидії

Поняття «дезінформації». Канали поширення дезінформації. Типи неправдивої інформації.

Технології неправдивих повідомлень. Інструменти виявлення неправдивих повідомлень.

Види маніпуляцій. Маніпуляції з медіаданими. Маніпулювання новинами. Маніпулювання експертними оцінками. Маніпулювання повідомленнями. Маніпуляції з результатами досліджень. Пропаганда як інструментів інформаційного впливу. Способи протидії неправдивим повідомленням.

Список рекомендованих джерел:

Основний: 3 [с. 19, 43-60, 64-79], 4 [с. 97-102].

Додатковий: 7 [с. 87-90].

Інтернет-ресурси: 14, 15.

Тема 6. Комп’ютерна вірусологія

Загальні поняття про комп’ютерні віруси, історія їх виникнення та

розвитку. Загальні принципи функціонування комп'ютерних вірусів, їх розмноження. Класифікація комп'ютерних вірусів і принципи її побудови. Алгоритми роботи вірусів.

Файлові, завантажувальні (бутові) та файлово-завантажувальні віруси. Макровіруси та мережні віруси. Класифікаційний код вірусу. Резидентність, використання стелсалгоритмів, самошифрування та поліморфізм, використання нестандартних методів.

Шляхи розповсюдження шкідливого програмного забезпечення (ШПЗ), вектори атак. Типи шкідливого програмного забезпечення. Шпигунські програми (spyware). Симптоми зараження ШПЗ. Завантажувач (дропер/лоадер). Викрадач інформації «інфостілер або стілер». Keylogger "кейлогер". «JS-сніфери». Троянські програми віддаленого доступу .rat. Банківські трояни (banking trojans). Ransomware (програма-вимагач, програма-шантажист). Майнери (miners). Шкідливе програмне забезпечення для знищення інформації без можливості її відновлення. Рекламне шкідливе програмне забезпечення (adware).

Список рекомендованих джерел:

Основний: 3 [с. 170-211].

Додатковий: 7 [с. 69-96].

Інтернет-ресурси: 14, 15.

Тема 7. Соціальна інженерія

Поняття соціальної інженерії. Методи соціальної інженерії. Види атак соціальної інженерії. Претекстінг (pretexting). Тейлгейтінг (tailgating). Послуга за послугу (quid pro quo). Злам пароля WI-FI. Атаки грубої сили (brute-force attacks). Прослуховування мережі (network sniffing). Фішингова атака. Етапи атаки із використанням СІ. Розвідка та збір інформації із відкритих джерел. Легендування та планування атаки із використання методів СІ.

Використання вразливостей як розповсюджений метод проникнення для отримання інформації.

Список рекомендованих джерел:

Основний: 2 [с. 112-148], 3 [с. 83-91].

Додатковий: 6 [с. 136-140], 7 [с. 8-25].

Інтернет-ресурси: 14

Тема 8. Соціотехнічна безпека: проблемні аспекти

Соціальна інженерія як метод розвідки складних соціальних і соціотехнічних систем: основні аспекти, поняття та визначення.

Особливості захисту сучасної інфосфери в умовах стороннього кібернетичного впливу. Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки. Соціальні мережі: особливості, основні поняття та визначення. Моніторинг соціальних мереж − цілі та способи реалізації. Поняття соціотехнічної системи та її властивостей. Системний підхід як загальнометодологічний принцип створення складних соціотехнічних систем.

Список рекомендованих джерел:

Основний: 2 [с. 64-95].

Додатковий: 6 [с. 144-159], 7 [с. 97-99].

Інтернет-ресурси: 14

Тема 9. Безпека спілкування в кіберпросторі

Захист інформації в глобальних мережах. Характер проведення атак у глобальних мережах. Захист під час використання WWW (World Wide Web).

Безпечне користування мережею «Інтернет». Найпоширеніші способи нелегального заробітку в мережі «Інтернет». Безпека браузерів. Безпека даних. Безпечне користування мережами WI-FI. Основні правила безпечного користування WI-FI. Безпечне користування месенджерами.

Список рекомендованих джерел:

Основний: 2 [с. 24-43].

Додатковий: 6 [с. 495-508], 7 [с. 41-52].

Інтернет-ресурси: 14

Тема 10. Особливості економічної діяльності суб'єктів господарювання в кіберпросторі

Безпека користування соціальними мережами. Реєстрація. Стійкий пароль. Оновлення паролів та парольних фраз. Конфіденційність даних. Налаштування конфіденційності та інших питань безпеки.

Безпека мобільних пристроїв**.** Блокування доступу до пристрою. Безпечна робота в мультимедійних засобах спілкування. Передавання вживаних мобільних пристроїв іншим особам. Передавання контактної інформації іншим особам. Вірусне програмне забезпечення. Додаткові функції мобільного пристрою. Головні правила роботи з мобільними пристроями.

Безпека користування електронною поштою. Конфіденційність електронної пошти. Найвідоміші атаки через електронну пошту. Загрози під час користування поштовою скринькою. Легітимні та фішингові листи

(investigation). **З**абезпечення безпеки особистої поштової скриньки (рекомендації).

Список рекомендованих джерел:

Основний: 2 [с. 130-147], 4[с. 35-49, 68-70].

Додатковий: 7 [с. 55-67, 97-99, 105-123].

Інтернет-ресурси: 14

Тема 11. Безпека цифрового простору суб'єктів господарювання

Технічні канали витоку інформації. Способи несанкціонованого зняття інформації з технічних каналів її витоку. Класифікація каналів витоку інформації. Методи та засоби блокування технічних каналів витоку інформації.

Системи та засоби виявлення, пошуку та знешкоджування технічних засобів зняття інформації. Захист акустичної інформації від зняття радіопристроями. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами. Захист інформації від несанкціонованого запису звукозаписувальними пристроями. Захист електронної інформації. Захист письмової інформації від оптичного зняття.

Список рекомендованих джерел:

Основний: 2 [с. 151-181], 3 [с. 43-60, 290-305].

Додатковий: 7 [с. 123-127].

Інтернет-ресурси: 14

Тема 12. Безпека Інтернету-речей

Історія Інтернету-речей. Екосистема Інтернету-речей. Архітектура Інтернету-речей. Технології Інтернету-речей. «Розумний та безпечний будинок».

Анатомія кібератак на IoT-пристрої. Mirai. Stuxnet. Ланцюжкова реакція. Туманні технології.

Криптографія. Симетрична криптографія. Асиметрична криптографія. Криптографічний хеш (аутентифікація і цифровий підпис). Інфраструктура відкритого ключа. Блокчейн і криптовалюта в Інтернеті-речей. Рекомендації щодо захисту IoT-пристроїв.

Список рекомендованих джерел:

Основний: 2 [с. 163-167].

Додатковий: 6 [с. 398-404, 480-482], 9 [с. 15-18, 111-127, 159-170, 189-200].

Інтернет-ресурси: 14

Тема 13. Системи захисту інформації на проникнення

Технології захисту на основі програмного забезпечення. Апаратні засоби захисту. Мережні технології захисту. Хмарні технології захисту.

Фізична безпека. Загрози, пов’язані з недотриманням правил фізичної безпеки. Найпопулярніша атака через фізичне втручання: Stuxnet.

Захист інформації за допомогою міжмережних екранів.

Маскування даних. Технології маскування даних. Стеганографія, основні терміни та визначення. Історичні приклади стеганосистем. Галузі застосування стеганографії. Методи та моделі стеганографії. Комп'ютерна і цифрова стеганографія, цифрові водяні позначки. Практичні аспекти побудови стеганосистем. Приховування даних у текстових файлах: методи текстової стеганографії; аналіз реалізації методів.

Список рекомендованих джерел:

Основний: 1 [с. 188-205], 2 [с. 158-159], 3 [с. 290-312].

Додатковий: 7 [с. 123-127].

Інтернет-ресурси: 14

Тема 14. Основні методи забезпечення кібербезпеки суб’єкта господарювання

Типи контролю доступу. Контроль фізичного доступу. Системи розмежування логічного доступу. Адміністративний контроль доступу.

Стратегії контролю доступу. Дискреційне розмежування доступу. Контроль доступу на основі ролей. Розмежування доступу на основі правил.

Ідентифікація. Управління ідентифікацією та доступом. Методи аутентифікації. Багатофакторна аутентифікація. Аутентифікація на основі одноразових паролей. Строга аутентифікація. Криптографічні протоколи строгої аутентифікації. Біометрична аутентифікація користувача. Авторизація. Використання авторизації.

Типи засобів контролю безпеки. Превентивні засоби контролю. Стримуючі засоби контролю. Ефективні механізми розкриття порушень. Коригуючі засоби контролю. Засоби відновлення. Компенсуючі засоби контролю.

Криптографія і її основні поняття. Модель криптографічної системи. Принцип Керкхоффса. Етапи розвитку криптографічних систем. Види історичних шифрів.

Типи шифрування. Шифрування за допомогою закритого ключа. Процес симетричного шифрування. Типи криптографічних перетворень.

Симетричні криптосистеми шифрування. Алгоритм шифрування DES, 3-DES. Стандарт шифрування AES. Основні режими роботи блочного симетричного алгоритму.

Список рекомендованих джерел:

Основний: 1 [с. 188-193, 205-210], 3 [с. 318-348].

Додатковий: 6 [с. 398-411, 480-491].

Інтернет-ресурси: 14

5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с. ISBN 978-617-582-069-8

2. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.− К.: ДУТ, 2015.− 288 с.

3. Безпека інформаційних систем: навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ: Держ. торг.-екон. ун-т, 2022. – 376 с.

4. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

Додатковий

5. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с.

6. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під. ред. В. М. Богуша. — К.: Видавництво Ліра-К, 2020. — 554 с. ISBN 978-617-7844-54-8.

7. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікатної) програми підвищення кваліфікації: Практикум. – Київ: ВАІТЕ, 2021. – 106 с.

8. Грабар І. Г. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія / І. Г. Грабар, Р. В. Грищук, К. В.

Молодецька; за заг. ред. д.т.н., проф. Р. В. Грищука. – Житомир: ЖНАЕУ, 2019. – 280 с.

9. Технології інтернету речей. Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 12,5 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с.

10. Указ Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 року "Про Стратегію кібербезпеки України" (дата звернення: 30.06.2022).

11. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради України, 2017. – № 45. – Ст.403 (дата звернення: 30.06.2022).

12. Закон України «Про оборону України» // Відомості Верховної Ради України. – 2017. – № 45. – Ст.403 (дата звернення: 30.06.2022).

13. Основи інформаційної безпеки: навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

Інтернет-джерела

14. Cisco -Україна. URL: https://www.cisco.com (дата звернення: 30.06.2022).

15. Annual Threat Reports. URL: https://www.fireeye.com/current-threats/annual-threat-report.html (дата звернення: 30.06.2022).

16. European union agency for cybersecurity. URL: https://www.enisa.europa.eu. (дата звернення: 30.06.2022).

**Курсивом зазначені джерела, що є в наявності в бібліотеці ДТЕУ*