dComFra

Digital competence framework for Ukrainian teachers and other citizens

598236-EPP-1-2018-1-LT-EPPKA2-CBHE-SP

Навчальна програма

Модуль M07 – Інформаційна безпека

Версія 0.2

Дата: 10 липня 2020 року

Розроблено:

к.т.н., доцент Палій Сергій Володимирович
доцент кафедри інформаційних систем і технологій
Київського національного університету
імені Тараса Шевченка

к.т.н., доцент Бронін Сергій Вадимович
доцент кафедри інформаційних систем і технологій
Київського національного університету
імені Тараса Шевченка

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

.

Модуль 07 – Інформаційна безпека

У цьому документі описано такі аспекти інформаційної безпеки: безпечне використання інформаційно-комунікаційних технологій (ІКТ) у повсякденному житті, а також поняття, які потрібні для забезпечення захищеного мережевого зв'язку, безпечного використання Інтернету та керування даними і інформацією.

Навички та вміння

Здобувачі, що успішно опанують усі теми модуля, зможуть:

- Розуміти ключові поняття, що стосуються інформаційної безпеки.
- Розуміти важливість збереження даних, знати загальні принципи захисту даних, забезпечувати та контролювати конфіденційність даних.
- Знати основні методології та стандарти інформаційної безпеки.
- Визначати загрози власній безпеці від крадіжок особистих даних.
- Розуміти потенційні загрози для даних при використанні хмарних технологій.
- Вміти використовувати паролі та шифрування для захисту файлів і даних.
- Розуміти загрози зловмисного програмного забезпечення та вміти захищати від них мережі, комп'ютери та інші пристрої.
- Розуміти загальні принципи мережевої безпеки та вміти користуватися персональними брандмауерами.
- Вміти захищати комп'ютери та інші пристрої від несанкціонованого доступу та керувати паролями.
- Розуміти, як безпечно переглядати веб-сторінки, вміти налаштовувати веб-браузер.
- Розуміти загрози використання електронної пошти, соціальних мереж, мобільних пристроїв, передачі голосу через Інтернет та обміну миттєвими повідомленнями.
- Створювати резервні копії у локальних та хмарних сховищах, відновлювати дані з резервних копій, безпечно видаляти дані та знищувати носії.

Загальна інформація

Рівень модуля:	проміжний
Мова:	українська, англійська
Облікове навантаження:	3 кредити ЄКТС
Орієнтовні часові затрати:	
- Змішана форма	9 днів по 8 годин на день
- Дистанційна	до 15 тижнів по 3-4 години в тиждень
Сертифікація:	Заключний екзамен

Попередні & рекомендовані модулі

Сертифікати за наступними модулями:

- M01 Computer Essentials;
- M02 Online Essentials.

Зміст модуля

ТЕМА 1 ОСНОВНІ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Загрози безпеці даних

- Дані та інформація.
- Кіберзлочинність. Портрет кіберзлочинця.
- Випадкові та зловмисні загрози.
- Загрози при надзвичайних ситуаціях.
- Загрози при використання хмарних обчислень.
- Загрози при застосуванні IoT та туманних обчислень.

1.2 Важливість захисту інформації

- Тріада інформаційної безпеки: конфіденційність, цілісність, доступність.
- Захист особистої інформації: уникнення крадіжок персональних даних, збереження конфіденційності, запобігання шахрайству.
- Захист інформації на робочому місці. Убезпечення при використанні концепції BYOD. Запобігання крадіжок даних, випадкової втрати даних, саботажу.
- Загальні принципи захисту даних та конфіденційності: прозорість, законність, пропорційність.
- Суб'єкти даних та контролери даних. Застосування до них принципів захисту даних, конфіденційності та контролю.
- Рекомендації та політики використання ІКТ.

1.3 Безпека особистих даних

- Поняття соціальної інженерії. Несанкціонований доступ до комп'ютерів та інших пристроїв, несанкціонований збір інформації, шахрайство.
- Методи соціальної інженерії: телефонні дзвінки, фішинг, "серфінг через плече" та "дайвінг у смітнику".
- Крадіжка особистості та наслідки. Види особистостей: приватна, кримінальна, фінансова, податкова, медична. Клонування особистості. Синтетична особистість.
- Методи крадіжки особистих даних, такі як: інформаційний дайвінг, скиммінг, претекстінг.

1.4 Безпечне збереження файлів

- Керування налаштуваннями безпеки макросу.
- Шифрування даних. Безпечне зберігання паролів, ключів, сертифікатів шифрування.
- Шифрування файлів, папок, дисків.
- Захист паролем текстових документів, електронних таблиць, архівів.

ТЕМА 2 ЗЛОВМИСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

2.1 Класифікація

- Типи зловмисного програмного забезпечення.
- Трояни, руткіти, бекдори, віруси, хробаки.

	▪ Використання зловмисного програмного забезпечення для отримання прибутку: рекламне програмне забезпечення, програми-вимагачі, шпигунське програмне забезпечення, ботнети, кейлогери, дайлери.
2.2 Захист від зловмисного програмного забезпечення	▪ Антивірусне програмне забезпечення та його обмеження. ▪ Важливість регулярного оновлення програмного забезпечення - операційної системи, антивірусних баз, браузерів, плагінів. ▪ Сканування дисків, папок, файлів за допомогою антивірусного програмного забезпечення. Сканування за розкладом. ▪ Ризики використання застарілого програмного забезпечення: збільшення ризиків, несумісність.
2.3 Ліквідація наслідків впливу зловмисного програмного забезпечення	▪ Переміщення в карантин заражених або підозрілих файлів. ▪ Видалення заражені або підозрілих файлів. ▪ Виявлення та нейтралізація атаки зловмисного програмного забезпечення за допомогою Інтернет-ресурсів: антивіруси, сайти підтримки операційної системи, постачальник браузера, сайти відповідних органів.

ТЕМА 3 БЕЗПЕКА В КОМП'ЮТЕРНИХ МЕРЕЖАХ

3.1 Локальні мережі та підключення мереж	▪ Класифікація мереж: локальні мережі (LAN), бездротові локальні мережі (WLAN), глобальні мережі (WAN), віртуальні приватні мережі (VPN). ▪ Технології підключення до мереж та безпека: несанкціонований доступ до даних, забезпечення конфіденційності. ▪ Автентифікація, авторизація та облік. ▪ Важливість регулярного встановлення патчів безпеки та оновлень. ▪ Моніторинг мережевого трафіку, робота зі зловмисним програмним забезпеченням. ▪ Використання брандмауера.
3.2 Безпека в бездротових мережах	▪ Параметри бездротового зв'язку: WEP, WPA, WPA2, MAC, SSID. ▪ Вразливості бездротових мереж: сніфери, викрадення мережі, "людина посередині". ▪ Убезпечення особистої точка доступу. Налаштування безпечного доступу та надійного підключення бездротових пристроїв.

Тема 4 Управління доступом

4.1 Методи управління доступом	▪ Заходи запобігання несанкціонованому доступу до таких даних: ім'я користувача, пароль, PIN-код, шифрування, багатофакторна автентифікація. ▪ Використання разового пароля. ▪ Мережевий обліковий запис. ▪ Доступ до мережевого облікового запису з використанням ім'я користувача та пароля. ▪ Необхідність виходити з системи. ▪ Біометричні методи контроля доступу.
4.2 Управління паролями	▪ Політики паролів: довжина пароля, використання літер, цифр та спеціальних символів, втаємничення паролів, регулярна заміна паролів, різні паролі для різних служб. ▪ Програмного забезпечення для керування паролями.

Тема 5 Безпечне використання веб

5.1 Налаштування веб-браузера	▪ Налаштування автозаповнення та автоматичного збереження при заповненні форми. ▪ Видалення приватні дані з браузера: історія перегляду, історія завантажень, кеш Інтернет-файлів, паролі, файли cookie, автозаповнення даних.
5.2 Безпечний перегляд веб-сторінок	▪ Деяка діяльність в Інтернеті (купівля, банківська справа), яку необхідно здійснювати виключно на захищених веб-сторінках з використанням захищеного мережевого з'єднання. ▪ Способи підтвердження автентичності веб-сайту: якість контенту, справжність URL-адреси, інформація про власника, контактна інформація, сертифікат безпеки, перевірка власника домену. ▪ Фішінг та фармінг. ▪ Функції та типи програмного забезпечення для управління вмістом: фільтрування в Інтернеті, батьківський контроль.

Тема 6 Комунікації в Інтернеті

6.1 Електронна пошта	▪ Шифрування електронної пошти. ▪ Цифровий підпис. ▪ Шахрайська електронна пошта, небажана електронна пошту, фішиг в електронних листах. ▪ Заохочення розкриття особистої інформації. ▪ Необхідність повідомляти про спроби фішингу легітимній організації та відповідним органам.

	▪ Небезпека зараження шкідливим програмним забезпеченням при відкритті вкладення електронної пошти, що містить макрос або файл для виконання.
6.2 Месенджери	▪ Вразливості Інтернет месенджерів (IM) та сервісів передачі голосу через IP (VoIP). ▪ Забезпечення конфіденційності під час використання месенджерів: шифрування, нерозголошення важливої інформації, обмеження спільного використання файлів.
6.3 Соціальні мережі	▪ Вважливість нерозголошення конфіденційної чи особистої інформації на сайтах соціальних мереж. ▪ Потенційні небезпеки під час використання сайтів у соціальних мережах: кібер-булінг, грумінг, зловмисне розкриття особистого контенту, фальшиві особистості, шахрайські чи зловмисні посилання, контент або повідомлення. ▪ Необхідність застосовувати та регулярно перевіряти налаштування конфіденційності облікових записів у соціальних мережах. ▪ Необхідність повідомляти про неналежне використання або поведінку соціальної мережі постачальнику послуг, відповідним органам.
6.4 Мобільний зв'язок	▪ Загрози використання програм не з офіційних магазинів додатків. ▪ Потенційна крадіжка приватних даних з мобільного пристрою: контактні дані, історія місцезнаходжень, зображення. ▪ Запобіжні заходи на випадок втрати мобільного пристрою: віддалене відключення, віддалене видалення даних, відслідковування місцезнаходження пристрою.

ТЕМА 7 УПРАВЛІННЯ БЕЗПЕКОЮ ДАНИХ

7.1 Захист даних	▪ Способи фізичного убезпечення комп'ютерів та пристроїв: постійний нагляд, використання тросів-блокаторів. ▪ Логування місцезнаходження обладнання, контроль доступу.
7.2 Резервне копіювання даних	▪ Важливість процедури резервного копіювання на випадок втрати даних з комп'ютерів та інших пристроїв. ▪ Особливості процедури резервного копіювання: регулярність та частота, графік, місце зберігання копій, компресія даних. ▪ Створення резервної копії даних: на локальному накопичувачі, на зовнішньому диску / носії інформації, в хмарному сервісі. ▪ Відновлення даних з резервної копії.

7.3 Безпечне видалення даних та знищення носіїв

- Різниця між видаленням даних та незворотнім видаленням даних.
- Необхідність незворотного видалення даних з накопичувачів або пристроїв.
- Видалення даних не може бути остаточним для таких сервісів: сайт соціальної мережі, блог, Інтернет-форум, хмарний сервіс.
- Загальні методи незворотного видалення даних: подрібнення, знищення накопичувача або носія, розмагнічування, використання спеціальних утиліт для незворотного знищення даних.