**Календарне планування з інформатики. 11 клас**

**(3 години на тиждень, 80 – на рік)**

***(80 години) І семестр – 32 год. / ІІ семестр – 48 год.***

***Викладач – Соменко О.О.***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Тема** | **Очікувані результати****навчально-пізнавальної діяльності**  | **Дата** | **Корекція/ Примітки** |
| **ІІ семестр****ВИБІРКОВИЙ МОДУЛЬ****Основи електронного документообігу****Тема 1. Документи та документообіг** |
|  | Поняття документу. Призначення та класифікація документів. Документообіг. Загальні правила оформлення документів.Стиль ділового листування. Логічні елементи тексту та порядок його викладення. | **Знаннєва складова**Знає поняття документа та документообігу.Пояснює що таке оригінал документа та його копія, підписувач, адресат, посередник.Описує обов’язкові реквізити документа.Називає загальні правила оформлення документів.Наводить приклади стандартів та уніфікованих систем документації.**Діяльнісна складова**Використовує правила оформлення сторінки.Створює бібліографічні списки та покажчики.Виконує правила та вимоги оформлення письмової роботи. Вміє використовувати шаблони та формуляр-зразки документа.**Ціннісна складова**Визначає логічні елементи тексту та дотримується порядку його викладення.Дотримується правил та вимог оформлення письмової роботи.Враховує стандарти документів та документообігу.Усвідомлює важливість документообігу. | **19.01****2 год. Лк** |  |
|  | Шаблони та формуляр-зразки документа. Реквізити документа. Правила оформлення сторінки. | **21.01****2 год. лк** |  |
|  | Практична робота №2.1 «Використання шаблону та формуляр-зразка документа»Оформлення бібліографічних списків та покажчиків.Правила та вимоги оформлення письмової роботи | **26.01****2 год. пз** |  |
|  | Практична робота №2.2 «Створення бібліографічних списків та покажчиків» Стандарти та уніфіковані системи документації. Системи управління електронними документами. | **02.02****2 год. пз** |  |
| **Тема 2. Технічні та програмні засоби обробки документів та інформації** |
|  | Технічні засоби обробки документів та інформації. Класифікація офісної техніки.Засоби створення, зберігання, обробки, копіювання і транспортування документів. | **Знаннєва складова**Знає основні технічні та програмні засоби обробки документів та інформації. Пояснює що таке системи управління електронним документообігом. Описує основні процедури створення електронних документів. Наводить приклади програмних засобів обробки електронних документів. (програми текстового редагування, системи обробки текстів, програмні видавничі системи) Називає найбільш поширені формати файлів електронних документів.**Діяльнісна складова**Використовує технічні та програмні засоби для створення, редагування, друку та пересилання документів. Створює прості текстові документи, вміє їх зберігати, копіювати та пересилати. Вміє виконувати маніпулювання електронними документами**Ціннісна складова**Визначає технічні та програмні засоби обробки електронних документів. Дотримується правил використання технічних засобів для роботи з документами, правил створення, зберігання, обробки і транспортування документів. Враховує призначення та можливості офісної техніки. Усвідомлює важливість використання технічних та програмних засобів обробки документів та інформації | **09.02****2 год. Лк****09.02 2 год. Лк** |  |
|  | Програмні засоби обробки документів та інформації. Види систем обробки текстів.  | **16.02****2 год. Лк****16.02 2 год. лк**  |  |
|  | Практична робота №2.3 «Створення та пересилання документів» Комунікаційні технології. | **23.02****2 год. пз** |  |
| **Тема 3.** Електронний документообіг |
|  | Електронний документ, його ознаки та правовий статус. Електронний документообіг. Електронний цифровий підпис.Особистий та відкритий ключі. Сертифікат відкритого ключа. OCR-технології для розпізнавання паперових документів.Виконання індивідуальних та колективних проектів. | **Знаннєва складова**Знає поняття електронного документа, електронного офісу та електронного документообігу. Описує основні процеси електронного документообігу. Називає основні вимоги до зберігання електронних документів. Наводить приклади електронних документів. Знає порядок електронного документообігу відповідно до законодавства України. Пояснює правовий статус електронних документів, їх реквізити. Пояснює що таке особистий ключ, відкритий ключ, сертифікати відкритого ключа їх термін дії. Знає які обов’язкові дані містить сертифікат ключа.Знає основні правила забезпечення конфіденційності електронних документів**Діяльнісна складова**Виконує основні процедури роботи з електронними документами (набір тексту, редагування, коректура, ілюстрування, макетування сторінок, друк) Використовує технічні та програмні засоби для створення, редагування, друку та пересилання електронних документів, забезпечення їх конфіденційності. Створює текстові документи, вміє їх зберігати, копіювати та пересилати. Вміє виконувати маніпулювання електронними документами в електронному офісі.**Ціннісна складова**Визначає ознаки та правовий статус електронних документів. Дотримується правил електронного документообігу із забезпеченням конфіденційності документів. Враховує та використовує правила роботи з електронними документами. Усвідомлює важливість використання електронного документообігу та створення електронного офісу | **02.03****2 год. лк** |  |
|  | Передавання електронних документів. Зберігання електронних документів. Забезпечення конфіденційності електронних документів. Електронний офіс.Практична робота №2.4 «Маніпулювання електронними документами»Захист проектів.**Тематичне оцінювання****Контрольна робота № 1** | **09.03****2 год. пз** |  |
| ВИБІРКОВИЙ МОДУЛЬІнформаційна безпекаТема 4. Основи безпеки інформаційних технологій |  |
|  | Основні поняття в області безпеки інформаційних технологій. Місце і роль автоматизованих систем в управлінні бізнес-процесами. Основні причини загострення проблеми забезпечення безпеки інформаційних технологій. Інформація та інформаційні відносини. Суб'єкти інформаційних відносин, їх інтереси та безпека, шляхи нанесення їм шкоди. Безпека інформаційних технологій. | **Знаннєва складова**Знає основні поняття інформаційної безпеки. Називає технічні та програмні засоби для несанкціонованого добування інформації. Наводить приклади вразливостей та загроз у інформаційних та комунікаційних системах.**Діяльнісна складова**Використовує програмні засоби для тестування та очищення операційної системи від вірусів та шкідливого програмного забезпечення. Виконує аналіз рівня захищеності операційної системи.**Ціннісна складова.**Дотримується правил мережного спілкуванняПоважає права інших користувачів на конфіденційність збереження даних. Усвідомлює відповідальність за збереження власних даних | **16.03****2 год. лк** |  |
|  | Загрози безпеці інформації в автоматизованих системах. Основні джерела і шляхи реалізації загроз безпеки та каналів проникнення і несанкціонованого доступу до відомостей та програмного коду. Основні ненавмисні і навмисні штучні загрози.Технічні засоби добування інформації. Програмні засоби добування інформації | **23.03****2 год. лк** |  |
|  | Практична робота №2.5 «Використання програмних засобів для тестування та очищення операційної системи від вірусів та шкідливого програмного забезпечення» | **30.03****2 год. пз** |  |
|  | **Тема 5. Забезпечення безпеки інформаційних технологій** |
|  | Об'єкти захисту. Види заходів протидії загрозам безпеки. Переваги та недоліки різних видів заходів захисту. Основні принципи побудови системи безпеки інформації в автоматизованій системі. | **Знаннєва складова**Знає основні методи і засоби захисту інформаціїПояснює суть технічного та криптографічного захисту інформації.Описує процес керування доступом в інформаційних системахНазиває міжнародні стандарти інформаційної безпеки.Наводить приклади видів засобів захисту інформаційних технологій**Діяльнісна складова**Використовує засоби адміністрування операційної системи для налаштовування прав користувачів щодо доступу до інформаційних ресурсів.Створює (змінює) правила, які забезпечують безпеку операційних системиВиконує моніторинг стану безпеки операційної системи за допомогою системних журналів **Ціннісна складова**Визначає потенційні загрози інформаційній системіДотримується законодавства України, яке регламентує відносини суб'єктів в інформаційній сфері та захист інформаціїУсвідомлює відповідальність за порушення у сфері захисту інформації та неправомірного використання автоматизованих систем | **06.04****2 год. пз** |  |
|  | Правові основи забезпечення безпеки інформаційних технологій. Закони України та інші нормативно-правові акти, що регламентують відносини суб'єктів в інформаційній сфері та захист інформації. Відповідальність за порушення у сфері захисту інформації та неправомірного використання автоматизованих систем.Основні захисні механізми, які реалізуються в рамках різних заходів і засобів захисту. Ідентифікація та аутентифікація користувачів. Розмежування доступу зареєстрованих користувачів до ресурсів автоматизованих систем. Реєстрація та оперативне оповіщення про події безпеки. Криптографічні методи захисту інформації. | **13.04****2 год. пз** |  |
|  | Контроль цілісності програмних і інформаційних ресурсів. Виявлення атак. Захист периметра комп'ютерних мереж. Керування механізмами захисту. Міжнародні стандарти інформаційної безпекиПрактична робота №2.6 «Використання засобів адміністрування операційної системи для налаштовування прав користувачів щодо доступу до інформаційних ресурсів, створення (змінення) правил, які забезпечують безпеку операційних системи.» | **20.04****2 год. Пз****21.04****2 год. пз** |  |
| **Тема 6. Забезпечення безпеки комп'ютерних систем і мереж** |
|  | Проблеми забезпечення безпеки в комп'ютерних системах і мережах. Типова корпоративна мережа. Рівні інформаційної інфраструктури корпоративної мережі. Мережеві загрози, вразливості і атаки. Засоби захисту мереж.Призначення, можливості, і основні захисні механізми міжмережевих екранів (брандмауерів). Переваги та недоліки брандмауерів. | **Знаннєва складова**Знає критерії, на основі яких здійснюється фільтрація даних в мережах Описує можливості, і основні захисні механізми міжмережевих екранів (брандмауерівНазиває засоби захисту мережНаводить приклади мережевих загроз**Діяльнісна складова**Створює віртуальні приватні мережіВиконує налаштування засобів системного міжмережевого екрану(брандмауера).Використовує засоби моніторингу мережного трафікуВиконує конфігурування простих маршрутизаторівВиконує резервне копіювання ОС та даних користувачів**Ціннісна складова**Дотримується правил безпечної роботи в ІнтернетіВраховує наслідки несанкціонованого доступу до інформаційних систем та корпоративних мережУсвідомлює необхідність резервного збереження даних | **27.04****2 год. пз** |  |
|  | Основні захисні механізми: фільтрація пакетів, трансляція мережевих адрес, проміжна аутентифікація, відхилення скриптів, перевірка пошти, віртуальні приватні мережі, протидія атакам, націленим на порушення роботи мережевих служб, додаткові функції. Політика безпеки при доступі до мережі загального користування. Практична робота №2.7 « Створення віртуальних приватних мереж» | **11.05****2 год. Пз** |  |
|  | Системи аналізу вмісту поштового і веб-трафіку (електронна пошта і НТТР). Політики безпеки, сценарії і варіанти застосування і реагування. Віртуальні приватні мережі (VPN). Загрози, пов'язані з використанням VPN.Практична робота №2.8 «Налаштування засобів системного міжмережевого екрану(брандмауера).Виконання конфігурування простих маршрутизаторів. Резервне копіювання ОС та даних користувачів» | **18.05****2 год. пз** |  |
|  | Антивірусні засоби захисту. Загальні правила застосування антивірусних засобів в автоматизованих системах. Технології виявлення вірусів. Можливі варіанти розміщення антивірусних засобів. Антивірусний захист, як засіб нейтралізації загроз.Виконання індивідуальних та колективних проектів.**Тематичне оцінювання****Контрольна робота № 2** | **18.05****2 год. Пз** |  |
|  | Повторення навчального матеріалу за рік |  | **20.05 2 год. Пз** |  |
|  | Підсумковий контроль знань |  | **20.05 2 год. пз** |  |