Віктор Пасько,
доцент кафедри технічної кібернетики НТУУ «КПІ», кандидат технічних наук
Наталія Прокопенко,
головний спеціаліст Департаменту загальної середньої
та дошкільної освіти МОН України

ПРОГРАМА КУРСУ ЗА ВИБОРОМ «ОСНОВИ КОМП'ЮТЕРНОЇ БЕЗПЕКИ»

ПОЯСНЮВАЛЬНА ЗАПИСКА

Метою курсу за вибором *«Основи комп'ютерної безпеки»* є формування в учнів знань та вмінь, необхідних для кваліфікованого використання сучасних технологій, стандартів, протоколів та засобів комп'ютерної безпеки. *Завданнями* курсу є формування в учнів теоретичної бази, необхідної для безпечної роботи з комп'ютером, розвиток уміння використовувати й самостійно освоювати сучасні програмні й технічні засоби захисту інформації, а також надати практичні рекомендації та іншу корисну інформацію, необхідну для того, щоб гарантувати психологічну, моральну та фізичну безпеку дітей під час роботи за комп'ютером.

Програма складається з:

- *пояснювальної записки,* в якій визначено мету і завдання курсу, особливості організації навчально-виховного процесу, перелік програмно-технічних засобів, необхідних для успішної реалізації курсу, та критерії оцінювання рівня навчальних досягнень учнів;
- *змісту навчального матеріалу* та *вимог до навчальних досягнень учнів.*

Вивчення курсу планується протягом одного півріччя, по одній годині на тиждень. Особливістю курсу є те, що він вимагає наявності інтернет-з'єднання, а також наявності спеціального програмного забезпечення, яке вчителю слід попередньо встановити на всіх комп’ютерах учнів. Окремі питання курсу можна вивчати лише в режимі ознайомлення без комп'ютера.

Програма курсу розрахована на 17 навчальних годин і може викладатися в середніх навчальних закладах будь-якого профілю в 10-х або 11-х класах. Для успішного навчання за тематикою курсу учні повинні мати стійкі навички роботи з прикладними програмами в середовищі Windows. Після вивчення цього курсу в учнів повинен бути сформований необхідний мінімум знань, умінь, навичок, завдяки яким можна успішної використовувати технології і засоби захисту інформації, що зберігається на комп'ютері, а також технології захисті під час доступу до мережі Інтернет.

Курс має практичну спрямованість. Передбачено проведення 9 практичних робіт. Оцінка, одержана учнем за виконання практичної роботи, може вважатися тематичною оцінкою з відповідної теми курсу. Для виконання практичних завдань має відводитися не менше половини загального навчального часу.

Для навчально-методичного забезпечення курсу, крім відповідних підручники і навчальних посібників, потрібні такі технічні й програмні засоби:

1. Комп'ютерний клас з локальною мережею Windows та доступом до Інтернету з усіх учнівських комп'ютерів.
2. Веб-браузер.
3. Програма для роботи з електронною поштою.
3. Антивірусні програми.
4. Програма для шифрування/де шифрування файлів.
5. Брандмауер.
6. Пакет Norton Internet Security.

Критерії оцінювання рівня навчальних досягнень учнів

Рівень навчальних досягнень	Бал	Критерії оцінювання рівня навчальних досягнень учня
I. Початковий	1	**Учень:** • пояснює основні принципи, яких слід дотримуватися для безпечної та комфортної роботи за комп'ютером; • вказує на джерела шкідливого впливу комп'ютера на користувача; • називає основні об'єкти, які треба захищати в комп'ютерних системах та мережах, загрози і вразливості інформації; • вказує на канали поширення вірусів; • уміє запустити антивірусну програму та перевірити файл на наявність вірусів
	2	**Учень:** • дає визначення конфіденційності, доступності та цілісності інформації, наводить приклади їх порушення; • описує призначення антивірусних програм та принципи їх роботи; • уміє використовувати антивірусні програми, засоби захисту веб-браузера та програми електронної пошти; • знає відмінність між резервним копіюванням та архівацією файлів
	3	**Учень:** • наводить класифікацію загроз безпеці та вразливостей інформації; • дає визначення інтелектуальної власності, комерційної таємниці; • описує канали поширення вірусів та методи запобігання зараженню вірусами; • уміє настроювати параметри безпеки антивірусних програм та веб-браузера
II. **Середній**	4	**Учень:** • описує рівні захисту інформації в комп'ютерних системах та мережах; • описує принципи функціонування брандмауера; • описує технології пошуку вірусів; • характеризує засоби забезпечення безпеки операційних систем, методи ідентифікації та автентифікації; • аргументує необхідність використання цифрового підпису, засобів шифрування інформації, наводить приклади методів шифрування; • уміє застосовувати стратегію уникнення спаму та антиспамове програмне забезпечення
	5	**Учень:** • наводить приклади стандартів інформаційної безпеки; • дає визначення політики безпеки; • дає порівняльну характеристику антивірусних програм; • описує принципи керування доступом в операційній системі Windows; • характеризує симетричні та асиметричні алгоритми і системи шифрування; • уміє використовувати функції керування доступом в Windows; • уміє настроювати параметри безпеки операційної системи Windows та програм електронної пошти

III. Достатній	6	**Учень:** • описує використання методів соціального інжинірингу, деструктивні функції програмних закладень; • дає характеристику стандартів безпеки, наводить приклади симетричних та асиметричних крилтосистем та хешувальних функцій; • уміє налагоджувати параметри вбудованого брандмауера Windows
	7	**Учень:** • уміє знаходити в Інтернеті й завантажувати необхідну інформацію для оновлення програмних засобів захисту, а також використовує засоби резервного копіювання та архівації, розуміє принципи роботи та вміє застосовувати програму відновлення системи Windows XP
	8	**Учень:** • пояснює небезпеку, пов’язану із зображенням cookie-файлів; • уміє ефективно опрацьовувати системний журнал Windows, використовувати програму PGP для спілкування з іншими учнями за допомогою програм електронної пошти
	9	**Учень:** *уміє* налагоджувати засоби захисту персонального комптера, брандмауера Zoone Alarm, а також використовувати пакет утиліт Norton Internet Security
IV.Високий	10	**Учень:** *уміє:* • сформувати політику безпеки під час роботи в Internet; здійснювати захист комп’ютера за допомогою Центру гарантування безпеки Windows; • настроїти параметри та використовувати програму PGP для шифрування та дешифрування інформації; • настроїти параметри програмних засобів безпеки персонального комп’ютера у локальній мережі та використовувати їх
	11	**Учень:** • активно використовує широкий спектр прогрмного забезпечення, призначеного для захисту інформації, зокрема антивірусні програми, засоби захисту безпеки операційної системи, веб-браузера, поштової програми, програми шифрування; • самостійно освоює нові засоби захисту й нове програмне забезпечення; • постіно розширює та активно застосовує знання у галузі інформаційної безпеки
	12	**Учень:** має стікі системні знання в галузі теоріїї й практики використання засобів інформаційної безпеки, уміє забезпечити комплексний захист персонального комп’ютера від інформаційних загроз, пов’язаних з Інтернетом, в процесі виконання завдань проявляє творчий підхід.

ЗМІСТ НАВЧАЛЬНОГО МАТЕРІАЛУ ТА ВИМОГИ ДО НАВЧАЛЬНИХ ДОСЯГНЕНЬ УЧНІВ

(17 год; 1 год на тиждень; 1 год резервного часу)

Зміст навчального матеріалу	Навчальні досягнення учня
1. Безпечна та комфортна робота за комп'ютером *(1 год)* Джерела шкідливого впливу комп'ютера на користувача. Санітарно-гігієнічні вимоги до персональних комп'ютерів та до робочого місця. Організація робочого місця користувача комп'ютера ***Практична робота № 1.*** Організація робочого місця користувача комп'ютера	**Учень** *описує:* • санітарно-гігієнічні вимоги до персональних комп'ютерів та 1 до робочого місця користувача комп'ютера; • джерела шкідливого впливу комп'ютера на користувача та способи нейтралізації такого впливу
2. Основні поняття інформаційної безпеки *(2 год)* Основні об'єкти і типи інформації, які треба захищати в комп'ютерних системах і мережах, конфіденційність, доступність і цілісність інформації.	**Учень:** • називає об'єкти, які треба захищати в комп'ютерних системах; • описує можливі загрози безпеці інформації, методи захисту і інформації під час її зберігання та передавання, можливі загрози, пов'язані з роботою в мережі Інтернет, критерії і класи безпеки комп'ютерних систем;

Класифікація загроз безпеці та вразливостей інформації в комп'ютерних системах. Етичні й правові основи захисту інформації. Інтелектуальна власність, патенти і комерційна таємниця. Стандарти інформаційної безпеки. Поняття про соціальний інжиніринг. Політика безпеки	• наводить приклади систем, у яких треба захищати інформацію, використання методів соціального інжинірингу, загроз безпеці та вразливостей комп'ютерних систем; • пояснює особливості стандартів інформаційної безпеки, необхідність створення політики безпеки
3. Антивірусні програми та комплекси *(2 год)* Класифікація комп'ютерних вірусів. Життєвий цикл вірусу. Канали поширення вірусів та інших шкідливих програм. Технології пошуку вірусів Антивірусні програми. Запобігання зараженню вірусами ***Практична робота № 2.*** Настроювання параметрів антивірусних програм, перевірка й лікування файлів і дисків	**Учень:** • описує деструктивні функції програмних застосувань; • пояснює спосіб дії вірусів і хробаків; • описує призначення антивірусних програм, основні технології виявлення шкідливого програмного забезпечення, канали поширення вірусів; • класифікує віруси; • порівнює принцип дії троянських програм і хробаків; • порівнює функціональні можливості антивірусних програм; • наводить приклади вірусів, троянських програм та хробаків, деструктивних проявів вірусів, антивірусних програм; • уміє використовувати антивірусне програмне забезпечення
4. Засоби безпеки операційної системи Windows *XP* *(2год)* Засоби гарантування безпеки операційних систем Ідентифікація та автентифікація користувачів. Система аудиту. Керування користувачами системи ***Практична робота № 3.*** Настроювання параметрів локальної політики безпеки в систем Windows XP ***Практична робота № 4.*** Настроювання параметрів групової політики безпеки в системі Windows XP	**Учень:** • описує принципи керування доступом в операційній системі Windows; • описує методи ідентифікації та автентифікації, засоби керування доступом та їх використання; • використовує функції керування доступом до ресурсів системи Windows XP; • здійснює захист комп'ютера за допомогою Центру гарантування безпеки Windows; • розуміє інформацію, наведену в системному журналі Windows, та використовує її
5. Інтернет та інформаційна безпека *(4 год)* Загрози, що походять з Інтернету. Правила безпеки під час роботи в Інтернеті. Поняття брандмауера. Використання брандмауерів Windows XF та Zone Alarm. Керування безпекою в Interne Explorer. Захист від спаму ***Практична робота № 5.*** Настроювання параметрів брандмауера Zone Alarm та брандмауера Windows XP ***Практична робота № 6.*** Настроювання параметрів безпеки браузера Internet Explorer та поштової програми Outlook Express	**Учень:** • описує поширені способи проникнення хакерів до інформаційних систем, поширені різновиди інформаційних атак зловмисників, поняття спаму, поняття addware та spyware, поняття брандмауера, поняття захищеного сайту; • називає загрози безпеці дітей під час роботи в Інтернеті, сімейні правила безпеки під час роботи в Інтернеті, програмне забезпечення, призначене для блокування addware та spyware; • пояснює методи боротьби зі спамом, політику безпеки, що регламентує використання Інтернету, принцип дії брандмауера на локальному комп'ютері та в локальній мережі, небезпеку, пов'язану зі збереженням Cookie-файлів; • уміє настроїти брандмауери Windows XP та Zone Alarm, застосовувати стратегію уникнення надходження спаму та антиспам-мове програмне забезпечення; • уміє настроїти параметри безпеки браузера Internet Explorer: керувати зонами безпеки, завантаженням Cookie-файлів, обмеженням доступу й сертифікатами
6. Резервне копіювання та відновлення даних *(2 год)* Резервне копіювання та відновлення даних. Періодичність резервного копіювання. Збереження резервних копій. Програма відновлення	**Учень:** • пояснює мету й процес резервного копіювання даних; • уміє запускати програму відновлення системи Windows XP; • пояснює поняття точки відновлення та називає різновиди точок відновлення; • уміє створювати точки відновлення користувача та повертати систему до стану, що зафіксований раніше створеною точкою

системи Windows XP Створення точок відновлення й повернення до них ***Практична робота № 7.*** Використання програми відновлення Windows XP	відновлення
7. Криптографічні методи захисту інформації *(4 год)* Мета й застосування шифрування інформації. Класичні методи шифрування. Симетричні алгоритми. Потокові та блочні шифри. Асиметричні алгоритми. Хешувальні функції. Електронний цифровий підпис. Розподіл ключів шифрування. Функції програми шифрування PGP та її застосування. Утиліти безпеки. Шифрування графічних та звукових файлів ***Практична робота № 8.*** Одержання й використання цифрового підпису ***Практична робота № 9.*** Використання зашифрованих повідомлень під час електронного листування з однокласниками	**Учень:** • описує методи шифрування й дешифрування інформації; • пояснює відмінність між симетричними та асиметричними алгоритмами шифрування, принцип дії та використання хешувальних функцій, функції цифрового підпису, поняття криптографічної стійкості шифру, відмінність між потоковими й блочними шифрами; • наводить приклади шифрів заміни та підстановки, симетричних та асиметричних алгоритмів шифрування; • уміє настроїти параметри та використовувати програму PGP для шифрування й дешифрування інформації; • пояснює принцип дії електронного цифрового підпису; • уміє одержувати в центрі сертифікації цифровий підпис та використовувати його для підписування повідомлень і файлів