ПРОГРАМА КУРСУ ЗА ВИБОРОМ
“ОСНОВИ КОМП’ЮТЕРНОЇ БЕЗПЕКИ ”
ДЛЯ ОСНОВНОЇ ШКОЛИ

Автори:
В.П. Пасько
Н.С. Прокопенко

Пояснювальна записка

Метою курсу за вибором «Основи комп'ютерної безпеки» є формування в учнів важливої складової інформаційної культури — знань та умінь, 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, розвинення уміння використовувати й самостійно освоювати сучасні програмні і технічні засоби захисту інформації, а також надати практичні рекомендації і 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*, де описано мету й завдання курсу, особливості організації навчально-виховного процесу та перелік програмно-технічних засобів, необхідних для успішного проведення курсу;
- *змісту навчального матеріалу* та вимог до навчальних досягнень учнів;
- *додатків*, у яких наведено критерії оцінювання рівня навчальних досягнень учнів та список навчально-методичної літератури.

Курс розраховано на ведення протягом одного півріччя, по одній годині на тиждень, навчання за програмою курсу може проводитися також протягом 8–9 тижнів, по дві години 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, щоб організовувати їх роботу в групах так, щоби за кожним комп’ютером працювало не більше трьох учнів водночас. Крім того, окремі питання курсу можуть вивчатися лише в режимі ознайомлення, без комп’ютера.

Обсяг курсу становить 17 годин. Курс може викладатися в середніх навчальних закладах будь-якого профілю в 10 або 11 класі. Для успішного навчання за тематикою курсу учні повинні мати стійкі навички роботи з прикладними програмами в середовищі Windows. Після вивчення даного курсу в учнів повинен бути сформований необхідний мінімум знань, умінь і навичок, завдяки яким можна успішно використовувати технології і засоби захисту

інформації, що зберігається на комп'ютері, а також технології захисту під час доступу до мережі Інтернет.

Курс має практичну спрямованість: протягом 17 навчальних годин заплановано проведення 9 практичних робіт, які є найважливішою складовою курсу. Слід також зазначити, що для виконання практичних завдань учням має бути відведено не менше половини загального навчального часу.

Для науково-методичного забезпечення курсу окрім відповідних підручників і навчальних посібників необхідні 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.
4. Антивірусні програми.
5. Програма для шифрування/дешифрування файлів.
6. Брандмауер.
7. Пакет програм, призначений для комплексного захисту комп'ютера.

ЗМІСТ НАВЧАЛЬНОГО МАТЕРІАЛУ ТА ВИМОГИ ДО НАВЧАЛЬНИХ ДОСЯГНЕНЬ

(16 годин + 1година резервного часу; 1 година на тиждень)

Зміст навчального матеріалу	***Навчальні досягнення учнів***
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. ***Практична робота №1***. Організація робочого місця користувача комп'ютера.	***Учень*** • Описує санітарно-гігієнічні вимоги до персональних комп'ютерів та до робочого місця користувача комп'ютера. • Описує джерела шкідливого впливу комп'ютера на користувача та способи нейтралізації такого впливу. • Вміє організовувати робоче місце користувача комп'ютера
2. Основні поняття інформаційної безпеки (2 год.) Основні об'єкти та типи інформації, які необхідно захищати в комп'ютерних системах та мережах. Конфіденційність, доступність і цілістність інформації.	***Учень*** • Описує можливі загрози безпеці інформації; методи захисту інформації під час її зберігання та передавання; можливі загрози, пов'язані з роботою в мережі Інтернет; критерії і класи безпеки комп'ютерних

Зміст навчального матеріалу	*Навчальні досягнення учнів*
Класифікація загроз безпеці та вразливостей інформації в комп'ютерних системах. Етичні та правові основи захисту інформації. Інтелектуальна власність, патенти та комерційна таємниця. Стандарти інформаційної безпеки. Поняття про соціальний інженірінг. Політики безпеки.	систем. • Називає об'єкти, які необхідно захищати в комп'ютерних системах. • Наводить приклади систем, у яких необхідно захищати інформацію; використання методів соціального інженірінгу; загроз безпеці та вразливостей комп'ютерних систем. • Пояснює особливості стандартів інформаційної безпеки; необхідність створення політики безпеки.
3. Антивірусні програми та комплекси (2 год.) Класифікація шкідливих програм. Життєвий цикл та спосіб дії вірусів, хробаків і троянських програм. Канали розповсюдження 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	***Учень*** • Описує деструктивні функції програмних застосувань. • Пояснює спосіб дії вірусів і хробаків. • Описує призначення антивірусних програм; основні технології виявлення шкідливого програмного забезпечення; канали розповсюдження вірусів. • Класифікує віруси. • Порівнює принцип дії троянських програм і хробаків. • Порівнює функціональні можливості антивірусних

Зміст навчального матеріалу	*Навчальні досягнення учнів*
дисків.	програм. • Наводить приклади вірусів, троянських програм та хробаків; деструктивних проявів вірусів; антивірусних програм. • Вміє використовувати антивірусне програмне забезпечення.
4. Засоби безпеки операційної системи Windows XP (2 год.) Засоби гарантування безпеки операційних систем. Ідентифікація та автентифікація користувачів. Керування доступом до ресурсів. Центр гарантування безпеки Windows. Система аудиту. Керування користувачами системи. ***Практична робота №3.*** Настроювання параметрів локальної політики безпеки в системі Windows XP. ***Практична робота №4.*** Настроювання параметрів	***Учень*** • Описує принципи керування доступом в операційній системі Windows. • Описує методи ідентифікації та автентифікації користувача, 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

Зміст навчального матеріалу	*Навчальні досягнення учнів*
групової політики безпеки в системі Windows XP.	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 XP та Zone Alarm. Сімейні правила безпеки під час рооти в Інтернеті. Поняття addware та spyware. Способи захисту від небажаного та шпигунського програмного забезпечення. Керування безпекою в Internet Explorer. Поняття про cookie-файли. 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. • Вміє настроювати брандмауери Windows XP та Zone

Зміст навчального матеріалу	*Навчальні досягнення учнів*
	Alarm; застосовувати стратегію уникнення надходження спаму та антиспамове програмне забезпечення; • Вміє настроювати 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 системи Windows XP. Створення точок відновлення й повернення до них. ***Практична робота №7.*** Використання програми відновлення Windows XP.	***Учень*** • Пояснює мету й процес резервного копіювання даних. • Пояснює поняття точки відновлення та називає різновиди точок відновлення. • Вміє запускати програму відновлення системи Windows XP. • Вміє створювати точки відновлення користувача та повертати систему до стану, що зафіксований раніше створеною точкою відновлення.

Зміст навчального матеріалу	*Навчальні досягнення учнів*
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.*** Отримання 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. • Пояснює принцип дії електронного цифрового підпису. • Вміє настроювати параметри та використовувати програму PGP для шифрування й дешифрування інформації.

Зміст навчального матеріалу	*Навчальні досягнення учнів*
	• Вміє отримувати в центрі сертифікації цифровий підпис та застосовувати його для підписування повідомлень і файлів.

Додаток 1. Критерії оцінювання рівня навчальних досягнень учнів з курсу за вибором «Основи комп'ютерної безпеки»

Рівні навчальних досягнень	*Бали*	*Критерії оцінювання рівня навчальних досягнень учнів*
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 необхідно захищати в комп'ютерних системах та мережах, загрози і вразливості інформації.
	2	• Учень дає визначення конфіденційності, доступності та цілістності інформації та дає приклади їх порушення; описує призначення антивірусних програм та принципи їх роботи; вміє запускати антивірусні програми, та використовувати 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 розповсюдження вірусів та методи запобігання зараженню вірусами; вміє запустити антивірусну програму, настроїти її параметри та параметри безпеки 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; вміє застосовувати стратегію уникнення спаму та антиспамове програмне забезпечення.

Рівні навчальних досягнень	*Бали*	*Критерії оцінювання рівня навчальних досягнень учнів*
	5	• Учень наводить приклади стандартів інформаційної безпеки; дає означення політики безпеки; дає порівняльну характеристику антивірусних програм; описує принципи керування доступом в операційній системі Windows; характеризує симетричні та асиметричні алгоритми та системи шифрування; вміє використовувати функції керування доступом в Windows; вміє настроювати параметри безпеки операційної системи Windows та програм електронної пошти.
	6	• Учень описує використання методів соціального інженірінгу, деструктивні функції програмних закладень; дає характеристику стандартів безпеки; наводить приклади симетричних та асиметричних криптосистем та хешувальних функцій; налагоджувати параметри вбудованого брандмауера Windows.
III.Достатній	7	• Учень вміє знаходити в Інтернеті й завантажувати необхідну інформацію для оновлення програмних засобів захисту, а також використовує засоби резервного копіювання та архівації. Учень розуміє принцип роботи та вміє застосовувати програму відновлення системи Windows XP.
	8	• Учень пояснює небезпеку, пов’язану із збереженням cookie-файлів; вміє ефективно опрацьовувати системний журнал Windows, використовувати програму PGP для спілкування з іншими учнями за допомогою програм електронної пошти.
	9	• Учень вміє налагоджувати засоби захисту персонального комп’ютера, брандмауера Zone Alarm, а також використовувати пакет утиліт Norton Internet Security.
IV.Високий	10	• Учень може сформувати політику безпеки під час роботи в Internet; здійснювати захист комп’ютера за допомогою Центру гарантування безпеки Windows; може настроювати параметри та використовувати програму PGP для шифрування та дешифрування інформації; вміє настроїти параметри програмних засобів безпеки персонального комп’ютера у локальній мережі та використовувати їх.

Рівні навчальних досягнень	*Бали*	*Критерії оцінювання рівня навчальних досягнень учнів*
	11	• Учень активно використовує широкий спектр програмного забезпечення, призначеного для захисту інформації, зокрема антивірусні програми, засоби захисту безпеки операційної системи, веб-браузера, почтової програми, програми шифрування; самостійно освоює нові засоби захисту й нове програмне забезпечення; постійно розширює та активно застосовує знання у галузі інформаційної безпеки.
	12	• Учень має стійкі системні знання в галузі теорії й практики використання засобів інформаційної безпеки, вміє забезпечити комплексний захист персонального комп'ютера від інформаційних загроз, пов'язаних з Інтернетом, в процесі виконання завдань проявляє творчий підхід.

Додаток 2. Перелік літератури

1. Інформатика. Програми для загальносвітніх навчальних закладів. – Запоріжжя: Прем'єр, 2003. – 304 с.
2. Державний стандарт загальної середньої освіти в Україні. Інформатика. Освітня галузь "Технології". – Київ, Освіта України. 2003.
3. Концепція загальної середньої освіти (12-річна школа). // Інформаційний збірник Міністерства освіти і науки України. Січень 2002. № 2.–Київ. Педагогічна преса. 2002.– 23 с.
4. В.Д. Руденко, О.М. Макарчук, М.О. Патланжоглу. Базовий курс інформатики. Книга 2. Інформаційні технології. — К., Видавнича група BHV, 2006 — 368 с.