*Грицун Ганна Володимирівна,*

*викладач інформатики та*

*інформаційних технологій*

*ВПУ № 17 м. Генічеська*

*Херсонської області*

**Тема програми: «**Інформаційні технології в суспільстві».

**Тема уроку:**«Проблеми інформаційної безпеки. Загрози при роботі в Інтернеті і їх уникнення».

**Мета уроку: формувати компетентності: *предметні* (***інформаційної культури та інформативної компетентності)*реалізація творчого потенціалу, соціалізація у суспільстві, ефективне використання засобів сучасних інформаційно-комунікаційних технологій; ***ключові компетентності:*** визначати основне поняття «інформаційна безпека», формувати вміння аналізувати інформацію, визначати основні загрози інформаційної безпеки користувача Інтернету, ознайомити учнів з правилами безпечної роботи в Інтернеті та принципами інформаційної безпеки;розвивати особистісно – смислового ставлення до навчального предмета, розвиток пам’яті, логічного мислення, предметного сприйняття, уваги;виховувати інтерес до вивчення інформатики, формування бережливого ставлення до обладнання комп’ютерного кабінету.

**Тип уроку:** комбінований.

**Методи навчання, прийоми:**вправа «Зірка», індивідуальна, групова, самостійна робота учнів, робота з електронним підручником, прийом «Відкрита трибуна», метод «Ланцюжок», тестування за допомогою « My Test Student».

**Форма організації навчальної діяльності учнів:** урок з використанням інтерактивних технологій.

**Основні терміни і поняття:**інформаційна безпека, конфіденційність, цілісність, доступність, хакерська атака, критичне мислення, спам, фішинг, шкідлива програма.

**Міжпредметні зв’язки:** історія, громадянська освіта, інформаційні технології.

**Наочність:**«Інформатика (рівень стандарту): підруч. Для 10(11)кл. Н.В.Морзе, О.В.Барна. «Оріон»,2018.-240с.:іл, роздатковий матеріал: схема: «Етапи розвитку засобів інформаційних комунікацій», схема «Принципи

гарантування інформаційної безпеки», схема « Види загроз».

**Технічні засоби навчання:**персональні комп’ютери.

**Програмне забезпечення:**ОCWindows, мережа Інтернет, браузер, програма MyTest.

**Хід уроку**

1. **Організаційний момент.**

Привітання учнів та перевірка готовності учнів до уроку.

1. **Перевірка домашнього завдання. Актуалізація опорних знань.**

**Вправа «Зірка»**

На дошці намальована зірка з центральним записом «Види інформації». Учні замість променів записують види інформації.

**Види**

**інформаційних**

**процесів**

**Види**

**інформації**

**Прийом «Відкрита трибуна»**

1. Як людина сприймає повідомлення? Наведіть приклади.
2. Що таке інформаційна система та якими є її складові?
3. Які інформаційні процеси можуть здійснювати власники сучасних мобільних телефонів?
4. **Формулювання теми, мети й завдань уроку, мотивація навчальної діяльності.**

**Слово викладача:**мережа Інтернет – одне з найвидатніших винаходів людства. Завдяки світовій павутині можна навчитися, шукати за допомогою електронних пошукових систем реферати, електронні книги, енциклопедії, здійснювати покупки, не витрачаючи час на походи до магазину. Інтернет для багатьох став засобом спілкування та зв’язку. Підключивши до персонального комп’ютера чи ноутбука веб-камеру, мікрофон та колонки, можна безкоштовно спілкуватися з людиною з іншого куточка світу та ще до того ж бачити співрозмовника на моніторі. Комп’ютерна мережа часто заповнює довкілля користувачів онлайн – фільмами, телебаченням та іграми.

Віртуальні подорожі, які кожен із вас здійснює, здавалося б не можуть загрожувати якимись серйозними небезпеками.Але ваша спокійна самотність за монітором оманлива, оскільки весь час, поки встановлене Інтернет - з’єднання, ваш комп’ютер є частиною величезної мереж і, де є і друзі, і вороги. Уберегтися від небезпеки завжди простіше, якщо знати, кого і чого боятися. Тому на цьому уроці ми розглянемо проблеми та принципи інформаційної безпеки, види загроз при роботі в Інтернеті та правила безпечної роботи в Інтернеті.

***Оголошення теми, мети та плану викладу нових знань.***

1. **Вивчення нового матеріалу.**

***Пояснення викладача:***

**Інформаційна безпека** – стан захищеності потреб людини, суспільства та держави в інформації незалежно від внутрішніх і зовнішніх загроз.

**Завдання для учнів:**

* розгадайте ребуси та визначте рівні захищеності інформаційного середовища.

(Й)

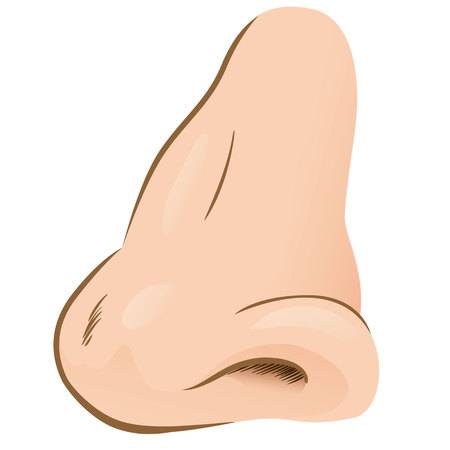
’’’ ‘ ‘ність.

*Очікувана відповідь(конфіденційність)*

Ці ’’’’ 

*Очікувана відповідь(*(цілісність)

ін

’’’ ’.

*Очікувана відповідь(*доступність)

***Самостійна робота учнів*.**

**Завдання:**

* Знайдіть в Інтернеті за допомогою нетбуків значення цих понять та запишіть у зошити.

*Очікувана відповідь:*

Під конфіденційністю розуміють забезпечення доступу до даних на основі розподілу прав доступу, захист від несанкціонованого ознайомлення.

Доступність означає забезпечення доступу до загальнодоступних даних усім користувачам і захист цих даних від блокування зловмисниками.

Цілісність передбачає захист даних від їх зловмисного або випадкового знищення чи спотворення.

***Слово викладача:***Інформаційна безпека держави характеризується ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т. д.) стосовно небезпечних (дестабілізаційних, деструктивних, суперечних інтересам країни тощо), інформаційним впливам, причому як до впровадження, так і до вилучення інформації.

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають.

Об'єктивно категорія «інформаційна безпека» виникла з появою засобів інформаційних комунікацій між людьми, а також з усвідомленням людиною наявності у людей і їхніх співтовариств інтересів, яким може бути завдано збитку шляхом дії на засоби інформаційних комунікацій, наявність і розвиток яких забезпечує і задає інформаційний обмін між всіма елементами соціуму.

***Індивідуальна робота учня:***

* Заздалегідь отримане завдання учнем «Етапи розвитку засобів інформаційних комунікацій».

***Очікувана відповідь:***

Етапи розвитку засобів інформаційних комунікацій

II етап — починаючи з 1816 року

IV етап — починаючи з 1946 року

III етап — починаючи з 1935 року

I етап — до 1816 року

VII етап — починаючи з 1985 року

VI етап — починаючи з 1973 року

V етап — починаючи з 1965 року

**Слово викладача:**Міжнародний день захисту інформації відзначається 30 листопада. З кожним роком його актуальність зростає через глобалізацію та повсюдне використання Інтернету. Сьогодні це поняття дещо трансформоване та охоплює більшу кількість проблем.

30 листопада 1988 вперше спостерігали за епідемією «хробака» («Морріс»), який показав, наскільки може бути вразливим персональний комп’ютер та інформація на ньому.

**Робота з електронним підручником.**

**Розділ 1**

* Пропоную для більш швидкої роботи з інформацією підручника скласти схему «Класифікація атак на комп’ютерні системи». (стор. 27 підручник для 10(11) кл. Н.В.Морзе, Оріон 2018)

**Слово викладача:**Зараз в Україні майже 22 млн. користувачів Інтернету, питання безпеки в мережі більш ніж актуальне. У цьому контексті турбота про дітей набуває більших масштабів. Якщо раніше треба було говорити з дітьми про їх безпеку поза домом тощо, то вже давно має сенс застерігати їх від негараздів під час перебування в Інтернеті.

**Групова робота учнів.**

**Завдання.**

* За допомогою нетбуків, користуючись мережею Інтернет та об’єднавшись в три групи, виконайте завдання.

**1 група** – Запишіть основні типи загроз, які стосуються особистої безпеки, безпеки інших, розвитку персональної інформації.

**2 група** – Захист держави, щодо забезпечення інформаційної безпеки.

**3 група** – Уникнення загроз під час роботи в Інтернеті.

**Слово викладача:**Інформаційна безпека стосується захисту життєво важливих інтересів людини (і більш глобально — суспільства, держави). Неправдива, неповна, невчасна інформація може нанести шкоду. Особливо вразливі у цьому контексті підлітки. Вони можуть не знати, яку інформацію можна викладати в мережу, а яку не варто. Інколи підлітки не можуть правильно зреагувати на матеріали з мережі з різних причин. Робота у цьому напрямку для викладачів та батьків дуже важлива. Безконтрольний доступ до інтернету може мати негативні наслідки для підлітка.

***Очікувані відповіді:***

***1 Група: «Типи загроз»***

***Слово викладача:***Це найбільш поширені типи загроз, з якими може зіштовхнутися підліток в Інтернеті, викладаючи чи переглядаючи сумнівну інформацію. Від деяких з них можна захиститися технічними засобами, але більшість вимагають комплексного підходу. Наприклад, у розібратися у цьому допоможе безкоштовний онлайн-курс від порталу Prometheus — [“Основи інформаційної безпеки”](https://edx.prometheus.org.ua/courses/KPI/IS101/2014_T1/about). Курс містить інформацію, яка буде цікава лише тим, хто захоплюється IT (історія появи вірусів). Але є й уроки, де розкриваються принципи захисту під час спілкування в соцмережах, при купівлі чогось в Інтернеті тощо.

***2 група – Захист держави, щодо забезпечення інформаційної безпеки.***

Для забезпечення захисту громадян кожна держава будує відповідну інформаційну політику щодо інформаційної безпеки.

В Україні політика гарантування інформаційної безпеки регламентується цілою низькою законодавчих актів, законів.

* Основним законодавчим актом в Україні, який регулює забезпечення захисту інформації, що належить особистості (громадянину), є Закон України « Про захист персональних даних».
* Конституція України, що стала гарантом побудови демократичної правової держави, не могла не врахувати загальносвітових тенденцій інформатизації суспільства. Тому ряд її статей (зокрема ст. 17, 32, 34) визначають забезпечення інформаційної безпеки, як одну з найважливіших функцій держави і мають стати основою розвитку інформаційного законодавства.
* Закон України “Про державну таємницю» січень 1994 року
* Концепція національної безпеки України
* Закони України “Про інформацію”
* Закон України “Про захист інформації в автоматизованих системах”

інші нормативно-правові акти, а також міжнародні договори України, що стосуються сфери інформаційних відносин

Всього, за нашими підрахунками, на сьогодні в Україні діє близько 60 нормативних актів, що стосуються регулювання відносин в інформаційній сфері. Крім того, видано низку відомчих актів Держкомсекретів України – циркулярних листів, роз’яснень, методик тощо (понад 15), які є обов’язковими для усіх державних органів, підприємств, установ, організацій під час здійснення ними функцій щодо забезпечення охорони інформації з обмеженим доступом, перш за все – державної таємниці.

Захист від хибної, викривленої, недостовірної інформації

Відповідальність за збереження інформаційних даних, її засекречування й розсекречування

**Принципи**

**гарантування інформаційної безпеки**

Контроль за створенням і використанням засобів захисту інформаційних даних

Регламентація прав, обов’язків і відповідальність всіх суб’єктів інформаційного простору

Забезпечення доступу до інформаційного ресурсу з урахуванням визначених Законом прав власності на цей ресурс.

***3 група – Уникнення загроз під час роботи в Інтернеті.***

Види загроз інформаційні безпеці.

Отримання несанкціонованого доступу до секретних або конфіденційних даних

Знищення та спотворення даних

Отримання несанкціонованого доступу до керування роботою комп’ютерної інформаційної системи

* Небажано розміщувати персональну інформацію в Інтернеті. Персональна інформація – це ваше повне ім'я, прізвище, номер мобільного телефону, адреса електронної пошти, домашня адреса, фото з вами, членами вашої родини, друзями.
* Не відповідайте на спам (небажану електронну пошту).
* Дотримуйтесь етики спілкування.
* Не розсилайте листи з будь-якою інформацією незнайомим людям без їхнього прохання - це сприймається як "спам", і звичайно засмучує користувачів мережі.
* Використовуйте тільки ліцензійне програмне забезпечення. Установлюйте програми тільки з офіційних джерел. Перед установленням читайте відгуки інших користувачів, якщо вони доступні.
* Установлюйте та оновлюйте антивірусне програмне забезпечення як на стаціонарні, так і на мобільні комп’ютери.
* Завжди встановлюйте оновлення операційної системи та іншого программного забезпечення.
* Використовуйтенадійніпаролі.
* Приєднуйтесятількидо перевіренихWi-Fi-мереж. Не відправляйтеважливідані через публічні та незахищеніWi-Fi-мережі.
* Установітьфільтрспливаючихвіконубраузері.
* Перевіряйтесертифікатбезпекисайтів у вигляді замка в адресному рядку браузера та URL-адреси веб-сайтів, щобвизначити,чи не підроблений сайт вивідвідуєте.
* Створюйтерезервнікопіїважливих для вас даних, зберігайтеїх на носіяхданих, відключенихвідмережіІнтернет.

**V. Первинне закріплення знань.**

**Дайте відповіді на запитання:**

1. Щотакеінформаційнабезпека?

2. Якіосновніскладовімаєінформаційнабезпека? Охарактеризуйте їх.

3. Наяківидиподіляютьсязагрозиінформаційній безпецізалежновід результату шкідливихдій?

4. Якізагрозиінформаційнійбезпецівиникаютьунаслідоккористування ресурсами Інтернету?

5. Яких правил потрібнодотримуватися, щобуникнутизагрозіінформаційнійбезпеціпід час роботи в Інтернеті.

**VI. Контроль і самоперевірка знань.**

***Робота з тестами за допомогою програми MyTestX.***

***Тест«Інформаційна безпека»:***

* 1. Захист інформаційних даних від несанкціонованого доступу:

1. Доступність;
2. **Конфіденційність;**
3. Цілісність.
   1. Дії кібер – зловмисників або шкідливої програми, спрямовані на захоплення, видалення або редагування інформаційних даних віддаленої системи, отримання контролю над інформаційними ресурсами системи або виведення її з ладу:
      1. Булінг;
      2. Фішинг;
      3. **Хакерська атака.**
   2. Віруси, які заражають файли Word, Excel:
4. Ретровіруси;
5. **Макровіруси;**
6. Panda Internet Securety.
   1. Прізвисько, псевдонім, який вибирає собі користувач Інтернету при спілкуванні в мережі Інтернет, називають…
7. **Нік;**
8. Логін;
9. Провайдер.
   1. Назвіть пристрій, що забезпечує взаємодію комп’ютера з лініями зв’язку:
10. Мережний адаптер;
11. **Модем;**
12. IP-телефонія.
    1. Віруси, які заражають антивірусні програми:
13. **Ретровіруси;**
14. Adware;
15. Макровіруси.
    1. Як називається поштова кореспонденція в основному рекламного характеру, що приходить на e-mail–адресу користувача без його запиту?
16. **Спам;**
17. Поштова бомба;
18. Фішинг.
    1. Вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів із переказування або обміну валюти, Інтернет – магазинів. Шахраї використовують усілякі виверти, які найчастіше змушують користувачів самостійно розкривати конфіденційні дані.
19. Спам;
20. **Фішинг;**
21. Комп’ютерні віруси.
    1. Забезпечення доступності інформаційних даних та основних послуг для користувача в потрібний для нього час:
22. **Доступність;**
23. Цілісність;
24. Конфіденційність.
    1. Служба призначена для обміну повідомленнями через електронні поштові скриньки:
25. Блог
26. Клавіатурний шпигун
27. **Електронна пошта**
    1. Коли вперше спостерігали епідемію «хробака» ( «Морріс»):
28. 25 листопада 1987 р.
29. **30 листопада 1988 р.**
30. 22 листопада 1986 р.
    1. Процес аналізу, синтезування й обґрунтування оцінки достовірності/цінності інформації; здатність генерувати чи змінювати свою позицію на основі фактів й аргументів, коректно застосовувати отримані результати до проблем і приймати зважені рішення.
31. **Критичне мислення**
32. Незалежність думок
33. Допитливість.

**VIІ. Підбиття підсумків уроку. Рефлексія.**

Повідомлення та обґрунтування оцінок.

Обговорімо, що ж нового ви дізналися на уроці, чи зможете в реальному житті застосувати отриманні знання.

**Метод «Ланцюжок».** Пропоную розпочинати висловлювання з формули:

* Про що ви дізнались на уроці…
* Використовуючи матеріал уроку, я зможу…
* Чи сподобався вам цей урок…

*«На дерево дивись, як родить, а на людину – як робить!»*

*(українськанародна мудрість)*

Я бажаю вам завжди працювати плідно, вірити в себе і завжди досягати поставленої мети. Це вам допоможе у подальшому дорослому житті.

**VІІI. Інформація, інструктаж домашньогозавдання.**

Створіть буклет або інформаційний бюлетень із правилами безпечної поведінки користувача в Інтернеті відповідно до обраної цільової аудиторії:

* школярі;
* студенти;
* працівники банківської сфери;
* будівники;
* викладачі.