17.02.2022

Урок 20-21

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

Мета уроку: формувати компетентності: ***предметні*** **(***інформаційної культури та інформативної компетентності)*реалізаціятворчого 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 інформаційних технологій, формування бережливого ставлення до обладнання комп'ютерного кабінету.

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 «Принципигарантування інформаційної безпеки», схема « Види загроз».

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

Завдання для здобувачів освіти:

- розгадайте ребуси та визначте рівні захищеності інформаційного середовища.

(Й)

,,,

‘

‘ність.

Очікувана відповідь(конфіденційність)

Ці   ,,,, 

 ,,,  ,   .

Самостійна робота здобувачів освіти.

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.

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.

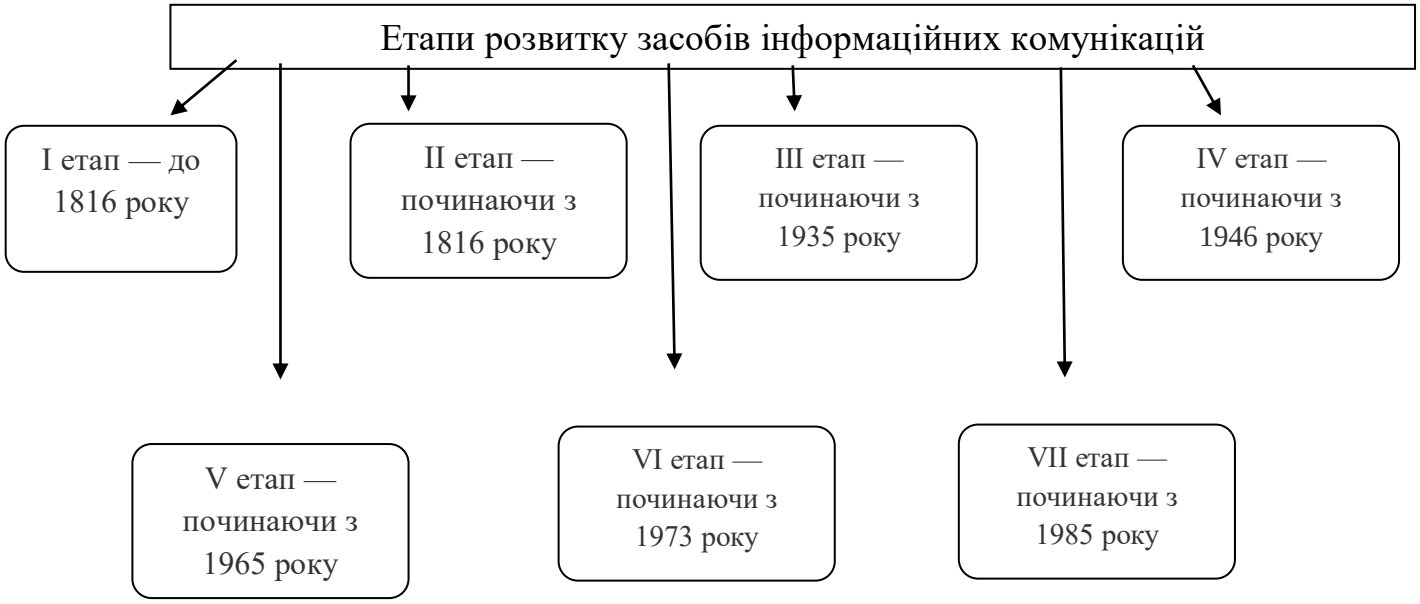
Об'єктивно категорія «інформаційна безпека» виникла з появою засобів інформаційних комунікацій між людьми, а також з усвідомленням людиною

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 здобувача освіти:

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

Очікувана відповідь:



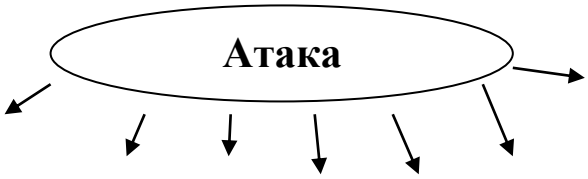
Міжнародний день захисту інформації відзначається 30 листопада. З кожним роком його актуальність зростає через глобалізацію та повсюдне використання Інтернету. Сьогодні це поняття дещо трансформоване та охоплює більшу кількість проблем.

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.

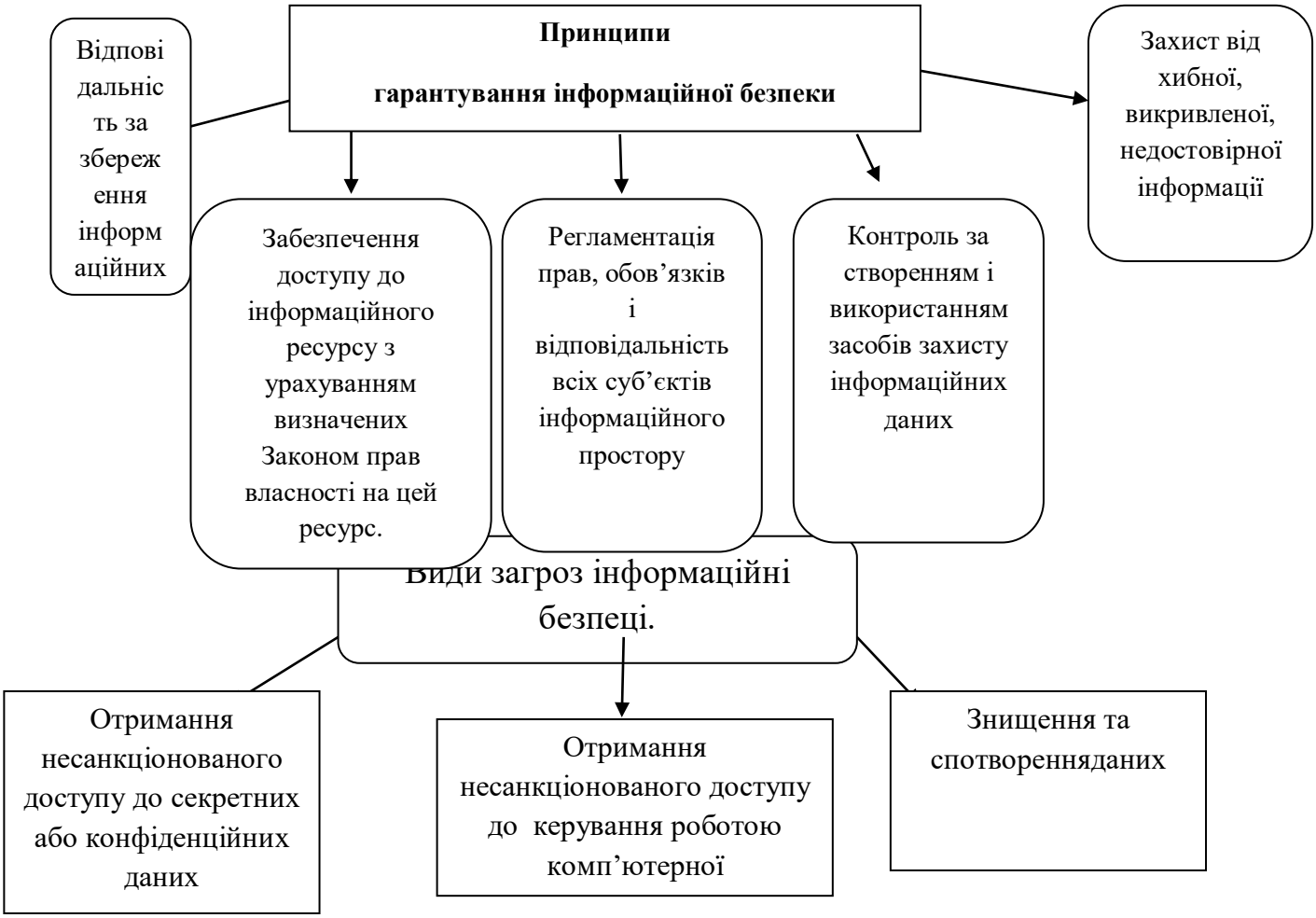
Розділ 1

- 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)



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.



- ✓ 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.

✓ Використовуйтетількиліцензійнепрограмнезабезпечення. Установлюйтепрограмитільки з офіційнихджерел. Перед установленням читайте відгукиіншихкористувачів, якщовонидоступні.

✓ Установлюйте та оновлюйтеантивіруснепрограмнезабезпечення як на стаціонарні, так і на мобільнікомп'ютери.

✓ Завждивстановлюйтеоновленняопераційноїсистеми та іншогопрограммногозабезпечення.

✓ Використовуйтенадійніпаролі.

✓ Приєднуйтесятількидо перевіреніхWi-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.

Установіть відповідність між терміном та його визначенням:

А. Конфіденційність	1. Дії кібер – зловмисників або шкідливої програми, спрямовані на захоплення, редагування чи видалення інформаційних даних віддаленої системи
Б. Цілісність	2. Стан, за якого потрібний інформаційний ресурс перебуває у вигляді, необхідному користувачеві, у місці, необхідному користувачеві, й у той час, коли він йому необхідний.
В. Доступність	3. Стан, за якого інформаційні дані не можуть бути отримані неавторизованим користувачем або процесом.
С. Хакерська атака	4.Захист точності та повноти інформаційних даних й програмного забезпечення.

Виконане завдання надсилати на адресу olia.dubina2017@gmail.com

У темі листа вказати номер груи, прізвище та ім'я.