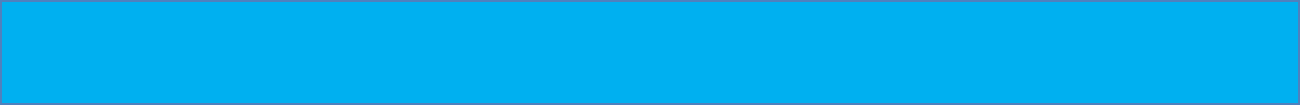


**МЕТОДИЧНИЙ КАБІНЕТ ВІДДІЛУ ОСВІТИ ПЕРВОМАЙСЬКОЇ РАЙДЕРЖАДМІНІСТРАЦІЇ**



**ІНФОРМАЦІЙНО-МЕТОДИЧНИЙ БЮЛЕТЕНЬ**

**2019**

****

**Методичний кабінет відділу освіти**

**Первомайської райдержадміністрації**

**Безпека дітей у глобальній**

**мережі Інтернет**

**Інформаційно-методичний бюлетень**

**2019**

Укладач: Волкова Н.П., методист методичного кабінету відділу освіти Первомайської райдержадміністрації

*Схвалено на засіданні науково-методичної ради РМК від 21.06.2019 р. (протокол № 2.).*

У бюлетені міститься інформація та загальні рекомендації для вчителів щодо формування в дітей компетенцій грамотного та безпечного використання Інтернет-ресурсів. Висвітлено способи безпечної поведінки дитини у віртуальному просторі, які убезпечать від негативного впливу на її психічне і фізичне здоров’я. Також подано конспекти уроків та сценарії проведення позакласних заходів з інформатики. Ці матеріали допоможуть відкрити дітям цікавий, корисний і, головне, безпечний Інтернет.

Бюлетень рекомендовано вчителям інформатики, класним керівникам.

«Безпека дітей у глобальній мережі Інтернет»

Волкова Н. П., П: РМК, 2019.- 70.

**ЗМІСТ**

Вступ…………………………………………………………………..……...5

**Частина І**

Інтернет-загрози для дітей………………………………………………..…7

10 золотих правил безпеки в Інтернеті для дітей…………………………14

Як захистити себе в інтернеті………………………………………………15

Шість правил розумного користувача Інтернету………………………....16

Поради батькам…………………………………………………………...…16

«Гарячі» контакти з Інтернет-безпеки………………………………..…....18

Використані джерела……………………….……………………………….21

**Частина ІІ**

*Мірянова Н.П.* Урок інформатики в 5 класі………………………………22

*Турова Р.А.* Суд над Інтернетом. Internet: глобальне добро чи зло?..........31

*Кулачинська Т.В.* Подорож океаном Інтернету…………………………....46

*Крохмальна О.А.* Подорож у світ Інтернету, або як Незнайко заплутався у всесвітній павутині………………………………………………………….55

**Вступ**

У свій час Цицерон сказав: «Не настільки прекрасно знати латину, як ганебно її не знати». Сьогодні це стосується інформаційно-комунікаційних технологій. У сучасному світі ІКТ є важливою і невід’ємною частиною держави, бізнесу та приватного життя. Тому впровадження ІКТ – один із пріоритетних напрямків сучасної освіти. Головною метою її розвитку є забезпечення загального доступу до освітніх ресурсів шляхом інтенсивного впровадження новітніх методів навчання, комп’ютеризації та інформатизації.

Сьогодні, з огляду на сучасні реалії, вчитель повинен використовувати нові методи роботи, спираючись на ІКТ. Це обумовлено тим, що в наш час кожні 72 години кількість інформації збільшується вдвоє, тому потрібні спеціальні навички, вміння та сучасні засоби для опрацювання такого величезного інформаційного об’єму. До того ж, сучасні діти народилися у цифровому світі ХХІ століття, тому з раннього віку знайомі з мобільними телефонами, ноутбуками, планшетами. Потужний потік нової інформації, реклами, застосування комп’ютерних технологій на телебаченні, розповсюдження ігрових пристроїв, електронних іграшок і комп’ютерів впливають на виховання дитини та сприйняття нею навколишнього світу. Істотно змінюється і характер її найпершої практичної діяльності – гри, змінюються й улюблені герої та захоплення. Тому дитина легко сприймає на уроці інформацію, подану за допомогою медіазасобів, оскільки вони є звичними та природними для неї.

Використання ІКТ у освітньому процесі дозволяє перейти від навчання, в основі якого – інформація, почута з вуст викладача або прочитана в підручнику, до навчання через сприймання інформації з електронних ресурсів, Інтернету, навколишнього середовища тощо. На будь-якому уроці вчитель, оперуючи різноманітними цифровими навчальними ресурсами, може організувати дослідницьку діяльність учнів, зорієнтувати індивідуальну роботу на поглиблений пошук інформації, навчити оцінювати надійність різних інформаційних джерел, створювати власні електронні продукти: малюнки, мультимедійні презентації, електронні моделі. Втрачає сенс необхідність перевантажувати ****пам’ять дитини великим об’ємом знань. Набагато важливіше навчити дитину знаходити інформацію і використовувати її на практиці, застосовувати в життєвих реаліях. Крім того, можливості, що відкриваються завдяки використанню ІКТ, дозволяють дітям навчатися в індивідуальному темпі, забезпечують ситуацію успіху для кожного учня, допомагають зробити процес здобуття знань захоплюючим і створюють міцну мотивацію до навчання.



Частина І

**Інтернет-загрози для дітей**

Інтернет – дуже потужний ресурс, який значно полегшує життя людини та відкриває майже необмежені можливості для самореалізації та саморозвитку юної особистості, спілкування, навчання, дозвілля. Але разом з тим в Інтернеті приховано досить багато небезпек як для дітей, так і для дорослих. Знання цих небезпек дозволить їх уникнути.

***Віруси***

Комп’ютерний вірус – це невелика програма, яка написана програмістом високої кваліфікації, здатна до самопоширення й виконання різних деструктивних дій. На сьогоднішній день відомо понад 50 тис. комп’ютерних вірусів. Дія вірусів може проявлятися по-різному: від різних візуальних ефектів, що заважають працювати, до повної втрати інформації. Більшість вірусів заражують виконавчі програми, тобто файли з розширенням .EXE та .COM, хоча останнім часом все більшої популярності набувають віруси, що розповсюджуються через систему електронної пошти.

Основними джерелами вірусів є:

- дискета, на якій знаходяться заражені вірусом файли;

- комп’ютерна мережа, в тому числі система електронної пошти та Інтернет;

* жорсткий диск, на який потрапив вірус у результаті роботи з зараженими програмами;

- вірус, що залишився в оперативній пам’яті після попереднього користувача.

Основними ранніми ознаками зараження комп’ютера вірусом є:

- зменшення обсягу вільної оперативної пам’яті;

- уповільнення роботи комп’ютера та завантаження;

- незрозумілі зміни у файлах, а також зміни розмірів та дати останньої модифікації файлів;

- помилки під час завантаження операційної системи;

- неможливість зберігання файлів у потрібних каталогах;

- незрозумілі системні повідомлення, музичні та візуальні ефекти тощо.

***Нелегальні та шкідливі матеріали, що не відповідають віковим особливостям і негативно впливають на фізичне та психічне здоров’я дітей (небажаний контент)***

*Контент для дорослих.* Понад 95% батьків вважають найголовнішою небезпекою «дорослий» контент, який можуть переглядати діти, зокрема інтимконтент. Розміри цієї індустрії неможливо навіть виміряти. Вона вважається третім великим джерелом прибутку для організованої злочинності в США, яка отримує від 8 до 10 більйонів доларів у рік. Інтернет може надати дітям швидкий та безкоштовний доступ до контенту. Необхідно лише ввести ключові слова або фрази для того, аби отримати тисячі посилань на сайти із дорослим контентом. Практично гарантовано, що дитина зіткнеться із інтимконтентом, навіть якщо вона і не шукала його.

*Онлайн-зваблення дітей.* Злочинці намагаються завоювати довіру дитини, щоб втягти її в ситуацію сексуального насилля. Варто зауважити, що в сучасних ЗМІ, а також в Інтернеті, пропагується сексуальність та навіюється думка, що значимість людини залежить від її сексуальної зовнішності та поведінки. Тобто людина розглядається як об’єкт втілення сексуальності. І злочинці цим користуються сповна. Знайомство та встановлення довіри між злочинцем і жертвою відбувається під час спілкування в мережі Інтернет: миттєві повідомлення, блоги, соціальні мережі, дошки оголошень та інше.

Діти не лише можуть легко знайти порнографічні сайти, вони так само легко можуть отримати інформацію, яка підштовхне до скоєння злочину, наприклад: інформацію про виготовлення та розповсюдження наркотиків, способи крадіжки грошей або про те, як зробити саморобну вибухівку. Необхідно лише набрати відповідну ключову фразу і – відповідь на екрані монітора!

***Кіберхуліганство***

Кіберхуліганство – термін, який використовується для того, аби описати інформаційні атаки на дитину через Інтернет. На відміну від традиційного хуліганства, якого дитина може уникнути, знаходячись вдома, стати жертвою кіберхуліганства можна й у власній оселі на очах у батьків. На жаль, багато дорослих навіть і не підозрюють про це. Варіанти кіберхуліганства досить різноманітні. Основними їх різновидами є наступні.

*Кібербулінг.* Одна із форм переслідування дітей та підлітків за допомогою ІКТ. Для цього можуть створюватися сайти, на яких розміщуються матеріали, що компрометують дитину (фото, відеозйомки тощо). З метою кібербулінгу використовуються сервіси миттєвих повідомлень, електронна пошта, соціальні мережі, ігрові та розважальні сайти, соціальні мережі, форуми та чати. Дорослі можуть здогадатися про кібербулінг по відношенню до своєї дитини, якщо стають свідками незвичної реакції на отримані електронні листи, СМС або помічають небажання дитини відвідувати школу чи використовувати домашній комп’ютер.

*Кібергрумінг.* Цей термін розкриває суть ще одного різновиду кіберхуліганства – входження у довіру до дитини з метою використання її у сексуальних цілях. Шахраї дуже добре ознайомлені з особливостями вікової психології дитини і досить легко можуть встановлювати з нею контакт у соціальних мережах, форумах. Починаючи із віртуального спілкування та входячи у довіру до дитини, злочинці пропонують потоваришувати, а потім поступово переходять до розмов про зустріч у реальному житті та переводять тему спілкування у сексуальну площину. Як варіант, виділяють ще один вид кібергрумінгу – наполегливе чіпляння в мережі із сексуальними пропозиціями, розмови на теми сексу, насильства або виготовлення, розповсюдження і використання матеріалів зі сценами насильства над дітьми.

*Грифери.* Інтернет-шахраї, які заважають учасникам онлайн-ігор спокійно грати. Вони періодично пошкоджують ігрових персонажів, блокують певні функції гри та викрадають як персонажів, так і їхнє віртуальне життя.

***Виманювання інформації про дитину та її сім’ю з метою подальшого пограбування, шантажу.***

*Шпигунське програмне забезпечення.* Це комп’ютерні програми, які збирають інформацію без відома власника комп’ютера. Зібрана інформація може містити:

- список рекламних сайтів, на які переходить користувач під час серфінгу в Інтернеті;

- особисту інформацію: ім’я, адресу та номер телефону;

-вебсторінки, які відвідує користувач, та відомості форм, які він заповнює на цих сторінках (треба пам’ятати про обережність при повідомленні паролів своєї електронної пошти та акаунтів у соціальних мережах; не слід називати дівоче прізвище матері – подібна інформація використовується при оформленні банківських документів у якості ключових слів);

- перелік файлів, які завантажує користувач на свій комп’ютер;

- інформацію, необхідну для доступу до Інтернету: номер з’єднання модему телефонної лінії, ID та інше.

Інтернет-зловмисники можуть використовувати шпигунське програмне забезпечення, аби одночасно встановити контроль над великою кількістю комп’ютерів та використовувати їх у якості зомбі.

Такі комп’ютери утворюють велику та потужну мережу, до якої можуть входити до 100 000 комп’ютерів. Ця мережа використовується шахраями для розсилання спаму, вірусів і здійснення атак на інші комп’ютери та сервери.

Фішинг – технологія інтернет-шахрайства, розроблена з метою крадіжки конфіденційної інформації. Різновидами її є поштовий фітинг (отримання листа від «державної установи» або «банку» із вимогою повідомити особисті дані) та онлайн-фішинг (створення ідентичної копії відомих сайтів Інтернет-магазинів з метою обманювання покупців).

*Фармінг.* Різновид шахрайства в інтернеті, коли оманливим шляхом користувач потрапляє на ідентичну копію відомих сайтів. Потім відбувається зараження комп’ютера вірусами та шпигунським програмним забезпеченням.

*Онлайн-хижаки.* «Хижаки» встановлюють контакт із дітьми шляхом розмов у чаткімнатах, обміну миттєвими повідомленнями, електронною поштою або через дошки повідомлень. Багато підлітків користуються онлайн-форумами підтримки ровесників з метою вирішення власних проблем. Хижаки часто відвідують такі зони в онлайні, щоб знайти вразливих жертв. Онлайн-хижаки виявляють по відношенню до них увагу та турботу, пропонують подарунки і таким чином намагаються поступово спокусити своїх жертв, не шкодуючи для цього ні часу, ні грошей, ні енергії. Вони в курсі найостанніших музичних новинок і все знають про хобі, які найчастіше цікавлять дітей. Вони вислуховують дітей і «співчувають» їхнім проблемам. Вони намагаються позбавити комплексів молодих людей, поступово вводячи у свої розмови сексуальний контекст або показуючи відверто сексуальні матеріали.

***Створення у мережі профайлів для виявлення інтересів дитини***

Як зазначалося вище, соціальні мережі набувають все більшої популярності у дітей та підлітків. Більшість існуючих соціальних мереж заохочують користувачів надавати якомога більше особистої та конфіденційної інформації (прізвище та ім’я, домашня адреса, номери телефонів, місце роботи, інтереси та нахили). Шахраю неважко обрати потенційну жертву та вивчити її за наданою у профайлі інформацією.

До речі, користувачі викладають подібну інформацію у більшості випадків добровільно, не усвідомлюючи можливих наслідків такої необережності. Діти охоче розміщують фотографії, які можуть також бути використані шахраями у своїх власних цілях. Іноді підлітки охоче розміщують свої пікантні фотографії, не замислюючись над тим, що опублікована в Інтернеті інформація залишається у мережі назавжди.

***Спам*** *–* цемасова розсилка комерційної, політичної та іншої реклами (інформації) або іншого виду повідомлень (у тому числі й підроблених) особам, які не висловлювали бажання їх отримувати. Фішинг також іноді може вважатися спамом. Метою розповсюдження підроблених повідомлень є отримання від споживачів таких особистих відомостей: власного імені та імені користувача; номера телефону й адреси; пароля або PIN-коду; номера банківського рахунку; номера дебетової або кредитної картки; коду валідації кредитної картки (CVC) або ідентифікаційного значення картки (CVV); коду соціального страхування.

Таке повідомлення, зазвичай, маскується під офіційний лист від адміністрації банку. У ньому говориться, що одержувач повинен підтвердити відомості про себе, інакше його рахунок буде заблоковано, і наводиться адреса сайту, що належить спамерам, з формою, яку треба заповнити. Серед даних, які просять повідомити, є ті, що потрібні шахраям. Для того, щоб жертва не здогадалася про обман, оформлення цього сайту також імітує оформлення офіційного сайту банку чи установи.

***Миттєві повідомлення.***З розвитком служб миттєвих повідомлень, таких, як ICQ тощо, спамери почали використовувати їх для своїх цілей. Багато з цих служб надають список користувачів, який можна використати для розсилання спаму.

***Блоги, вікі.*** Останнім часом з’явилися Web-сайти, які можна вільно редагувати, — блоги й вікі. Наприклад, Вікіпедія створена за цією технологією. Оскільки ці сторінки відкриті для вільного редагування, на них може розміщуватися спам.

***SMS-повідомлення.*** Спам може поширюватися не тільки через інтернет. Рекламні SМS-повідомлення, які надходять на мобільні телефони, особливо неприємні тим, що від них важче захиститися, і одержувач іноді повинен платити за кожне повідомлення. Це може бути досить велика сума, особливо якщо абонент використовує роумінг.

***Торгівля людьми.*** Враховуючи вищенаведені ризики, легко змоделювати декілька ситуацій в інтернеті, які можна використати з метою торгівлі людьми: від сайтів, що пропонують роботу (роботодавці можуть виявитися звичайними торговцями людьми), до шантажу з метою викрадення жертви та її подальшого продажу.

***Недостовірна інформація.*** Вчителі закладів ЗЗСО помітили, що якість шкільних рефератів протягом останніх років погіршилася: інформація, яка міститься у більшості рефератів, є недостовірною, неповною або застарілою. І це не дивно, адже учні завантажують вже готові реферативні повідомлення з Інтернету та роздруковують їх. Це займає часу максимум 1 годину. Проте часто учні не замислюються над достовірністю отриманої інформації, не вміють аналізувати та узагальнювати її, тому що у них відсутнє або недостатньо розвинуте критичне мислення.

Якщо при підготовці рефератів недостовірна чи неправдива інформація до життєвого ризику не призводить, то у випадку пошуку інформації, що стосується здоров’я, ризик істотно збільшується.

Проблеми, що стосуються здоров’я, як фізичного, так і психічного, повинні обговорюватися лише у родині, із дорослими та фахівцями. В інтернеті на різноманітних форумах досить легко знайти інформацію, яка є не лише антинауковою, а й життєво небезпечною, якщо нею скористатися.

***День безпечного Інтернету***

День безпечного Інтернету (SID) організовано мережами **Insafe та INHOPE** за підтримки Європейської комісії для просування ідеї відповідального використання онлайн-технологій та мобільних приладів, особливо дітьми та молоддю. Він відзначається на другий день другого тижня другого місяця щорічно. Тисячі людей в усьому світі об’єднуються та беруть участь у різних заходах заради підвищення освіченості з питань безпеки онлайн.

Безпечною онлайн-платформою для виховання коректної поведінки у мережі сьогодні є сайт «Онляндії» – [www.onlandia.org.ua](http://www.onlandia.org.ua). Сайт є основним ресурсом програми «Онляндія – безпека дітей в Інтернеті».

**10 золотих правил безпеки в інтернеті для дітей**

1. Нікому без дозволу батьків не давати особисту інформацію: домашню адресу, номер домашнього телефону, робочу адресу батьків, їхній номер телефону, назву й адресу школи.

2. Якщо знайдете якусь інформацію, що турбує вас, негайно сповістіть про це батьків.

3. Ніколи не погоджуватися на зустріч з людиною, з якою ви познайомилися в інтернеті. Якщо все ж таки це необхідно, то спочатку потрібно спитати дозволу батьків, а зустріч повинна відбутися в громадському місці й у присутності батьків.

4. Не посилати свої фотографії чи іншу інформацію без дозволу батьків.

5. Не відповідати на невиховані і грубі листи. Якщо одержите такі листи не з вашої вини, то сповістіть про це батьків, нехай вони зв'яжуться з компанією, що надає послуги інтернет.

6. Розробити з батьками правила користування інтернетом. Особливо домовитися з ними про прийнятний час роботи в Інтернеті і сайти, до яких ви збираєтесь заходити.

7. Не заходити на аморальні сайти і не порушувати без згоди батьків ці правила.

8. Не давати нікому крім батьків свої паролі, навіть найближчим друзям.

9. Не робити протизаконних вчинків і речей в інтернеті.

10. Не шкодити і не заважати іншим користувачам.

**Як захистити себе в інтернеті**

• Використовувати брандмауер (інші назви – мережевий екран, firewall) – програмне забезпечення чи пристрій, призначений для контролю над обміном даними між мережами чи мережею та окремою комп’ютерною системою. Він дозволяє встановити фільтр, що надає доступ лише безпечній інформації за встановленими параметрами.

• Користуватися лише ліцензійними програмами. А також не скачувати та не встановлювати неліцензійні програми з неперевірених сайтів.

• Слідкувати за станом свого комп’ютера: якщо він веде себе дивно (часто «зависає», повільно працює тощо) – це може означати, що він заражений вірусом.

• Встановлювати та своєчасно оновлювати на комп’ютері антивірусні програми, спамфільтри.

• Уважно ставитися до особистої інформації, яку розміщуєте в мережі (а краще зменшити до мінімуму). Не надавати ніяку інформацію незнайомцям та не йти на реальну зустріч з ними без згоди старших.

• Використовувати надійні паролі для доступу у електронну пошту, сторінок соцмереж, форумів та сайтів, які потребують реєстрації. Надійний пароль – той, який містить багато цифр та додаткових символів.

• Не записуйте паролі там, де їх можуть побачити інші особи (а краще просто запам’ятати) та не розказуйте нікому про них. Для кращого захисту потрібно також час від часу змінювати свої паролі.

• Після використання свого профіля в соцмережі натискати кнопку «вихід» перед закриттям сторінки (так буде менше шансів її зламати).

• Не натискати на спливаючі вікна. Як правило, закрити такі вікна можна лише натиснувши на позначку «Х», яка з’являється не одразу, або спеціально замаскована. Крім того, існують також спеціальні програми для блокування спливаючих вікон, які можна встановити.

• Не надавати дані банківських карток, сплачувати за послуги чи товари онлайн лише в присутності чи за допомоги старших осіб. Перевіряти також, чи існує в реальному житті той чи інший онлайн-магазин (чи має він, наприклад, адресу).

**Шість правил розумного користувача інтернету:**

1. Я буду поводитись в інтернеті чемно і не ображати інших.

2. Я буду залишати негарні вебсайти.

3. Я буду зберігати свій пароль в таємниці.

4. Я буду розповідати своїм батькам про проблеми й користуватися їхньою підтримкою.

5. Я буду шукати цікаві вебсайти й ділитися посиланнями зі своїми друзями.

6. Я знаю, що можна бути легко обманутим і не буду повідомляти реальні імена, адреси й номери телефонів.

**Поради батькам**

*Онлайн-ігри*

• Уважно спостерігайте за тим, чим займається ваша дитина і стежте за іграми, в які вона грає. Рольові ігри справляють найбільш сильний вплив на психіку. Надмірне захоплення рольовими іграми може негативно позначитися на формуванні особистості дитини, її соціалізації та рольовій ідентифікації, тому не дозволяйте їй тривалий час грати в одну гру.

• Якщо дитина любить грати в комп’ютерні ігри, можна запропонувати їй цікаві навчальні та розвиваючі програми. У випадку, коли інтерес дитини зосереджено на рольових іграх, можна привабити її участю в шкільних театральних виставах або психологічних тренінгах для підлітків.

• Коли дитина продовжує надмірно захоплюватися комп’ютерними іграми та інтернетом і ви не в змозі самостійно впоратися з проблемою, зверніться до спеціаліста-психолога.

*Для підвищення онлайн-безпеки вашої дитини:*

• Разом з дітьми розробіть правила користування інтернетом. Особливо домовтеся з ними про прийнятний час роботи в інтернеті і сайти, до яких вони збираються заходити.

• Знайдіть час для відвідування сайтів разом з дітьми та заохочуйте їх ділитися з вами знаннями, отриманими в інтернеті.

• Якщо діти спілкуються в чатах, використовують програми миттєвого обміну повідомленнями, грають або займаються чимось іншим, що вимагає реєстраційного імені, допоможіть дитині його вибрати і переконайтеся, що воно не містить ніякої особистої інформації.

 • Наполягайте на тому, щоб діти ніколи не видавали своєї адреси, номера телефону або іншої особистої інформації. Наприклад, місце навчання або улюблені місця для прогулянки.

• Навчайте дітей не розміщувати свої чи сімейні фотографії.

• Поясніть, що давати свої паролі не можна нікому, крім батьків, навіть найближчим друзям.

• Поясніть, що не потрібно відповідати на невиховані й грубі листи. Якщо отримали такі листи, то потрібно сповістити про це батьків чи вчителів.

• Скажіть дітям, що їм не слід зустрічатися з людьми, яких вони знають тільки з інтернету. Поясніть, що ці люди можуть виявитися зовсім не тими, за кого себе видають. Якщо ж це необхідно, то спочатку треба спитати дозволу батьків. Зустріч у громадському місці та й у присутності батьків.

• Скажіть дітям, що не все, що вони читають або бачать в інтернеті, – правда. Привчіть їх запитувати вас, якщо вони не впевнені.

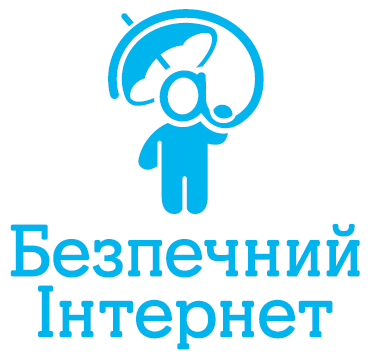
• Навчіть дітей поважати інших в інтернеті. Переконайтеся, що вони знають про те, що правила етикету діють скрізь – навіть у віртуальному світі.

• Наполягайте, щоб діти не завантажували музику, комп'ютерні ігри та інші програми без вашого дозволу.

• Поясніть, наскільки небезпечно для комп’ютера переходити на посилання, адреси яких вам невідомі.

• Контролюйте діяльність дітей в інтернеті за допомогою сучасних програм. Вони допоможуть відфільтрувати шкідливий вміст, з'ясувати, які сайти відвідує дитина і що вона на них робить.

Дотримуйтесь цих простих правил, і ви будете впевнені, що жодна людина з нечесними намірами не отримає доступу до вашої персональної інформації.

****«Гарячі» контакти з інтернет-безпеки**

*1. Спеціальний розділ сайту компанії «Київстар» із захисту дітей від негативного контенту.*

Проконсультуватися з експертом з онлайн-безпеки можна на сайті <http://online-bezpeka.kyivstar.ua>, де кваліфіковані спеціалісти дадуть відповіді на Ваші питання.

*2. Електронна гаряча лінія з протидії дитячої порнографії в інтернеті «Ла Страда-Україна».*

Повідомити про випадки дитячої порнографії в інтернеті можна за допомогою форми на головній сторінці <www.internetbezpeka.org.ua>.

Головною метою роботи ресурсу є блокування розповсюдження дитячої порнографії, особливо на серверах українських інтернет-провайдерів. Гаряча лінія функціонує на базі Міжнародного жіночого правозахисного центру «Ла Страда – Україна».

*3. Національна «гаряча лінія» з питань протидії домашньому насильству і захисту прав дітей.*

Звернувшись на гарячу лінію за телефоном 0 800 500 335 (безкоштовно для дзвінків із стаціонарних телефонів на території України), або 386 (безкоштовно для дзвінків з телефонів мобільних операторів «Київстар» і «МТС») чи електронною поштою на <info@lastrada.org.ua>, <onlandia@live.com>, можна одержати такі консультації:

• Правила безпечної поведінки дітей під час користування інтернетом.

• Поради батькам з безпечної роботи дітей в інтернеті.

• Попередження комп’ютерної залежності і можливість отримання психологічної допомоги.

• Юридичні консультації стосовно злочинів проти дітей в інтернеті.

• Допомога у випадках або підозрах загрози дітям через інтернет.

Гаряча лінія працює на базі Міжнародного жіночого правозахисного центру

«Ла Страда-Україна» за інформаційної підтримки проекту «Онляндія».

*4. Проект із протидії незаконним матеріалам в інтернет-просторі України Skarga.ua*

Кожний користувач українських інтернет-порталів може сповістити про матеріали, що порушують законодавство країни та містять порнографію з участю неповнолітніх, прояви расової і національної нетерплячості, вияви тероризму, заклики до насильницької зміни конституційного ладу за допомогою форми на головній сторінці <http://skarga.ua/>

*5. Телефон Довіри МВС України*

Телефон довіри Департаменту МВС: (+380 44) 254-76-04.

Повідомити про вебсайти, що пропагують насильство і жорстокість або розпалюють ненависть, расову дискримінацію, займаються створенням чи розповсюдженням дитячої порнографії можна в Департамент боротьби зі злочинами, пов’язаними з торгівлею людьми МВС України.

**Використані джерела**

1. Діти в Інтернеті: як навчити безпеці у віртуальному світі: посібник для батьків / І. Литовченко, С. Максименко, С. Болтівець [та ін.]. – К.: ТОВ «Видавничий будинок «Аванпост-Прим»», 2010. – 48 с. [Електронний ресурс]. – Режим доступу до методичного посібника: <https://rvo-kolomak.ucoz.ua/Informatizazija/kijiv_star.pdf>.
2. Виховання культури користувача Інтернету. Безпека у всесвітній мережі: навчально-методичний посібник / А. Кочарян, Н. Гущина. – К., 2011. – 100 с. [Електронний ресурс]. – Режим доступу до методичного посібника: [http://old.mon.gov.ua/images/newstmp/2011/18\_02/3/4press.pdf](http://old.mon.gov.ua/ua/activity/education/59/196/korinf19/bezditvinet/www.mon.gov.ua/images/newstmp/2011/18_02/3/4press.pdf).
3. Безпечне користування сучасними інформаційно-комунікативними технологіями / О. Удалова, О. Швед, О. Кузнєцова [та ін.]. – К.: Україна, 2010. – 72 с.
4. Пам’ятка для батьків «Діти. Інтернет. Мобільний зв’язок», розроблена Національною експертною комісією України з питань захисту суспільної моралі [Електронний ресурс]. – Режим доступу: <http://www.moral.gov.ua/news/311/>.
5. [Перелік рекомендованих для дітей онлайн-ресурсів](http://old.mon.gov.ua/education/pozashkilna/useful_information/internet/onl_resyrs/), затверджений на засіданні Національної експертної комісії України з питань захисту суспільної моралі (рішення від 20.04.2010 № 2).
6. Бугайова Н.М. Ризики сучасних комп’ютерних технологій: ігрова залежність.// Інформаційні технології в наукових дослідженнях і навчальному процесі: Матеріали II Міжнародної науково-практичної конференції, м. Луганськ, 14 – 16 листопада 2006 р. т.1. – Луганськ, 2006.
7. Українська молодь не може жити без Інтернету [Електронний ресурс] / Офіційний сайт інформаційного агентства УНІАН. – Режим доступу: <http://www.unian.ua/society/779261-ukrajinska-molod-ne-moje-jiti-bez-internetu-doslidjennya.html.>



Частина ІІ

***Мірянова Н.П., учитель інформатики***

***Кінецьпільської ЗОШ І-ІІІ ступенів***

**Клас:** 5

**Тема: Безпечне користування Інтернетом.**

**Мета:**

***формування предметної компетентності:*** уміння класифікувати небезпеки під час користування інтернетом та програмне забезпечення для їх уникнення; уміння користуватися службою WWW за допомогою браузера, відкривати вебсторінку шляхом уведення URL.

***формування ключових компетентностей:***

* інформаційно-комунікаційна компетентність (уміння протистояти загрозам, які існують в мережі; уміння користуватися засобами браузера, які призначено для гарантування безпеки, розуміння переваг користування захищеними сайтами);
* навчання впродовж життя (уміння самостійно приймати рішення щодо використання тих чи інших засобів захисту даних);
* громадянські та соціальні компетентності (навички перевірки правдивості інформації й до особистості співрозмовника; уміння розпізнавати прихований зміст повідомлень, протистояти шахрайству та маніпулюванню свідомістю людини);
* екологічна компетентність (уміння визначити чинники, що впливають на благополуччя людини, дотримання правил безпечної поведінки в інформаційному середовищі).

**Очікувані результати:** дотримуватись правил безпеки в інтернеті.

**Основні поняття:** безпечне використання інтернету, спам, вірус, онлайн та офлайн загрози.

**Обладнання**: ПК з виходом в мережу Інтернет, підручник, роздатковий матеріал.

**Тип уроку**: комбінований.

**Випереджальне завдання**: Підготувати повідомлення «Вірус та його ознаки», «Як запобігти онлайнове піратство вдома».

**Прийоми та методи:** слово вчителя,вправи: «Лови помилку», «Інтелектуальна розминка «На мою думку», «Будиночок з хмаринкою», робота за комп’ютером, робота у парах з інтерактивними вправами, вправа «Лавровий вінок».

**Перебіг уроку**

1. **Мотиваційний етап** 
   * + 1. ***Забезпечення емоційної готовності до уроку***

Усміхніться всім навколо:

Небу, сонцю, квітам, людям,

І тоді обов'язково

День і вам веселим буде!

Сідайте, будь ласка!

Сядьте рівно, поверніться,

Один одному всміхніться.

Пропоную на уроці побувати,

Гарний настрій один одному подарувати.

* + - 1. ***Актуалізація суб’єктного досвіду та опорних знань учнів***

**Вправа «Лови помилку».**

На картках записано групи слів. Учні викреслюють зайве поняття, обмінюються картками. Здійснюють взаємоперевірку.

* Папка, фрагмент тексту.
* Ім’я комп’ютера, вебсайт, гіперпосилання.
* Глобальна мережа, комп’ютер, локальна мережа, інтернет.
* Ключові слова, обліковий запис, пошук.
* Веббраузер, мережна папка, вебсайт.

**ІІ. Етап цілевизначення і проектування діяльності**

***Ознайомлення з темою і метою уроку***

*Слово вчителя.* Сьогодні ми продовжимо знайомство з Інтернетом та його можливостями. Із розвитком глобальної мережі Інтернет наш звичний спосіб життя дуже змінився. Ви з раннього віку знайомі з мобільними телефонами, ноутбуками, планшетами. Величезна кількість інформації чекає вас повсюди і дуже впливає на ваше сприйняття навколишнього світу. Ви легко сприймаєте інформацію, подану за допомогою медіа-засобів.

Як на вашу думку мережа Інтернет впливає на вас?

Так, мережа Інтернет має як позитивний, так і негативний вплив на наше життя.

У нас є доступ практично до будь-якої інформації, що зберігається на мільйонах комп’ютерів у всьому світі. Але, з іншого боку, мільйони комп’ютерів отримують доступ до нашого комп’ютера. І не сумнівайтеся, вони скористаються цією можливістю. І не колись, а прямо зараз. Крім того, незахищеність вашого комп’ютера може призвести до зараження його вірусами. Отже, тема нашого уроку: «Безпечне користування Інтернетом». Девізом нашого уроку пропоную обрати наступні слова: **«Віртуальний світ живе за своїми правилами – і ми повинні їх знати!».**

На уроці ви ознайомитеся та навчитеся користуватись правилами безпечної поведінки в Інтернеті.

**ІІІ. Опрацювання навчального матеріалу**

1. ***Розповідь вчителя з використанням мультимедійної презентації***

Інтернет ... Останні роки це слово щільно увійшло в наше життя. Це цікавий і захоплюючий світ, який дозволяє нам дізнаватися багато цікавого, спілкуватися з людьми, які живуть в різних кінцях світу, не виходячи з власної кімнати, грати в цікаві ігри і ділитися з іншими своїми думками і захопленнями. Сучасна людина не уявляє собі життя без Інтернету.

Коли ми потрапляємо до Всесвітньої мережі, ми потрапляємо в світ, де нас оточують люди: хороші і погані, добрі і злі, розумні і не дуже; інформаційні потоки: корисні і шкідливі; новини, музика; фільми і ще багато різної інформації. Ми свідомо здійснюємо пошук серед усього цього розмаїття. Інтернет є дуже широким джерелом інформації, іншими словами, інформаційним простором, в якому, як і в реальному житті, існують позитивні і негативні сторони.

1. ***Інтелектуальна розминка* *«На мою думку…»***

*Слово вчителя*. Пропоную висловити свою точку зору стосовно наступних висловлювань:

1. Інтернет – це глобальний рекламний ресурс. (І це …)

2. Інтернет має необмежені можливості дистанційної освіти. (І це …)

3. Спілкування в Інтернеті – це …, тому що дуже часто воно заміняє реальне.

4. У Інтернеті можна дізнатися відомості про людину (місце проживання і адреса електронної пошти, номер мобільного телефону).

5. Інтернет магазини – це…, тому що це найбільш популярний вид шахрайства в Інтернеті.

Сьогодні проблема безпеки дітей в Інтернеті в Україні стоїть особливо гостро. Аудиторія користувачів Всесвітньої мережі постійно розширюється, і її велику частину складають діти та підлітки, які не усвідомлюють повністю загроз, що можуть чекати на них у віртуальному просторі. Загрози, які виходять із мережі Інтернет, можна розділити на онлайн та офлайн.

Почнімо з першої групи загроз – онлайн-загрози. Онлайн-загрози – це будь-які проблеми, які небезпечні для вас і вашого комп’ютера в мережі. До них, по-перше, відносяться різні види комп’ютерних шкідників і вірусів, які можуть просочитися на ваш комп’ютер під час подорожі по просторах соціальних мереж. Для цього деколи досить натиснути на посилання, що містить в листі від «мнимого» друга. Наприклад, отримали лист або знайшли повідомлення на стіні такого змісту: «Знайшов твоє фото!», або «Ти тут непогано вийшла!». Зацікавившись змістом листа, ви натиснете на посилання, яка приведе вас на загадковий сайт, попутно завантажує на комп’ютер шкідливі програми.

Серед них можуть бути програми-шпигуни, які будуть відслідковувати ваші дії на комп'ютері, що вводиться з метою її викрадення.

1. ***Розповідь заздалегідь підготовлених учнів***.

Послухаємо ваших товаришів, які заздалегідь підготували повідомлення до сьогоднішнього уроку. (Повідомлення учнів за темами: «Вірус та його ознаки», «Як запобігти онлайн-піратству вдома?») (додаток 1).

1. ***Розповідь вчителя (продовження).***

А тепер перейдемо до найбільш небезпечного виду загроз, який може завдати шкоди не тільки вашому майну, а й життю – це онлайн-загроза. Вона включає все те, що може статися в реальному житті. До неї відносяться пропозиції про зустріч від невідомих «друзів», телефонний шантаж, шахрайство, вимагання і навіть пограбування квартири.

Найчастіше шахраям навіть не потрібно ламати голову над тим, як отримати заповітну інформацію від користувача – він сам надає її на тарілочці. Наприклад, при реєстрації в соціальній мережі і складанні особистого профілю пропонується внести інформацію про рік народження, номер телефону, адреса електронної пошти, адреса проживання. На жаль, люди часто сприймають такі «вимоги» як необхідність, і заносять особисту інформацію до всіх граф. Це перша і найголовніша помилка! Необхідно вносити якомога менше особистої інформації. Чому?

Ось простий приклад: дитина в очікуванні довгоочікуваних канікул з батьками і всією сім'єю в заморській країні кожен день оновлює статус в соціальній мережі: «Ура, до подорожі залишилося три дні!», «Залишилося два дні, не можу дочекатися!», а на третій-четвертий день, після того, як дні закінчилися, квартиру обкрадають. Причина в тому, що крім щоденного оновлення статусів дитина додав у профіль домашню адресу і фотографії з квартири, в якій шахрая, а вже і «грабіжника», зацікавив інтер'єр і домашня апаратура.

 Проблема безпеки дітей та молоді в мережі Інтернет дуже актуальна. Сьогодні в Україні діє профілактична програма «Онляндія – безпека дітей в інтернеті», яка включає цілий ряд заходів, спрямованих на навчання дітей, батьків та вчителів правилам безпечного користування мережевими ресурсами ([www.onlandia.org.ua](http://www.onlandia.org.ua)).

В Україні запущений спеціальний поштовий сервіс для дітей – безпечна електронна пошта «Онляндія», яка базується на безкоштовному вебсервісі Microsoft – Windows Live Mail.

 Інтерфейс поштового домену @onlandia.org.ua не містить реклами. Електронна скринька захищена від несанкціонованого спаму та вірусів. Є можливість не тільки надсилати електронні листи, а й спілкуватися з друзями в режимі онлайн за допомогою сервісу обміну миттєвими повідомленнями

***5. Фізкультхвилинка «Збери рукостискання».***

Учням пропонується протягом 10 секунд привітатися за допомогою рукостискання із якомога більшою кількістю однокласників.

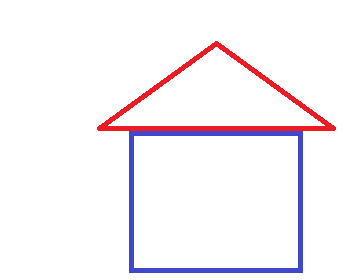
*Обговорення:*

- Кому скільки чоловік вдалося привітати?

- У когось виник психологічний дискомфорт?

- Якщо так, то чим він був викликаний?

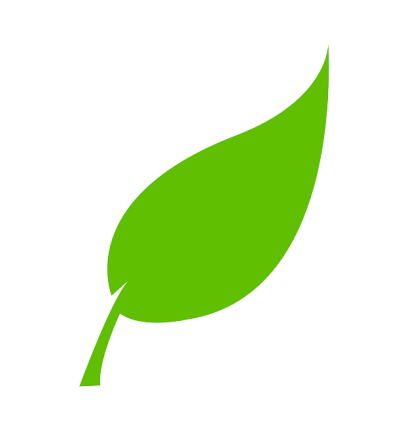
*Аналогія з роботою в інтернеті:*

** Спілкуючись в інтернеті, ми дуже часто додаємо незнайомих людей у свої соціальні мережі і спілкуємося з ними. Ми не знаємо про них абсолютно нічого, тільки їхні ніки. Як багато інформації про людину ми можемо дізнатися від віртуального імені або рукостискання?

***6. Вправа «Будиночок з хмаринкою».***

Діти придумують собі Нік і пишуть його на даху будиночка, який прикріплюють на малюнок. Далі пишуть побажання на хмаринці і прикріплюють її на будь-який будиночок. Після чого намагаються вгадати, де чий нік.

99% учнів не зможуть вгадати відправника повідомлення.

******Робимо висновок: Дуже важко перевірити, хто саме пише тобі листи, спілкується з тобою. Якщо нік вгадали, то робимо висновок: в інтернет-просторі не існує почерків, тому ми ніколи не знаємо, хто знаходиться по інший бік комп’ютера або смартфону.

***7. Практична робота.***

*Увага! Дотримуйтесь правил безпечної поведінки в кабінеті інформатики та ІКТ, а також правил охорони здоров'я та безпеки життєдіяльності при роботі за комп’ютерами!*

***Вправа 1. Гра «Перший мільйон»***

[**https://learningapps.org/display?v=p8mootqtv18**](https://learningapps.org/display?v=p8mootqtv18)

***Вправа 2.* *Безпечна поведінка в інтернеті***

Розподіли твердження, запропоновані у вправі за посиланням [**http://LearningApps.org/view1293380**](http://learningapps.org/view1293380), у дві групи: відповідають правилам безпечної поведінки в мережі Інтернет і не відповідають їм.

**Вправа 3**. ***Працюємо в парах***

Перегляньте відео за посиланням [**https://www.youtube.com/watch?v=zPIXOPDGRAY**](https://www.youtube.com/watch?v=zPIXOPDGRAY). Обговоріть і запропонуйте продовження списку правил поведінки розумного користувача інтернету*.* Звіт оформити у вигляді презентації з 1-2 слайди.

**ІV. Рефлексивно-оцінювальний етап**

*****Вправа «Лавровий вінок».***

Які правила безпечної роботи ви вибрали, відвідуючи веб-сайти? Сформулюємо 10 правил вашої безпечної поведінки в інтернеті.А зробимо ми це досить незвичним способом. На папері намальована заготовка лаврового вінка. З давніх давен відомо, що лавр – це ознака чистоти, а лавровий вінок – символ володарства, перемоги та тріумфу. Кожен із вас має заготовку «лаврового листа». Напишіть на ньому одне правило безпечної поведінки в мережі Інтернет, озвучте його та приклейте до вінка, і в результаті ми отримаємо наш лавровий вінок – символ тріумфального та безпечного використання вебресурсів.

***Оцінювання та цінування відповідей учнів.***

***Домашнє завдання***

Обов’язкове. 1. Опрацювати розділ 2, пункт 2.3, ст. 79–80.

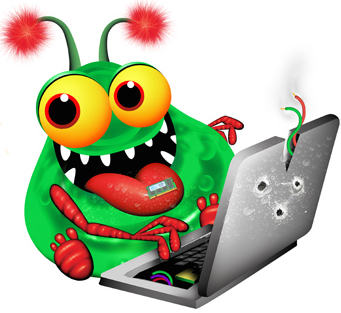
2. Відповісти на питання 1–3 ст. 84,

3. Вправа №2 ст. 84.

За бажанням. Підготувати пам’ятку «Моє безпечне перебування в мережі Інтернет».

**Додаток 1**

**Вірус та його ознаки**

 Вірус – це програма, яка виконує несанкціоновані дії, має руйнівну дію, а також здатна до саморозмноження з подальшим додаванням своїх копій до файлів, системних частин комп’ютера, і також на інші комп’ютери, об’єднані в мережу (причому дублікати зберігають здатність до подальшого самопоширення).

***Ознаки зараження вірусом можуть бути наступні:***

1. уповільнення роботи комп’ютера;
2. затримка при виконанні програм;
3. зміни в файлах;
4. зміна дати модифікації файлів без причини;
5. незрозумілі помилки;
6. помилки при інсталяції та запуску Windows;
7. неспроможність зберігати документи Word в інші каталоги, крім TEMPLATE;
8. погана робота дисків;
9. зникнення файлів;
10. неспроможність завантажити комп’ютер;
11. неспроможність завантажити файли;
12. незрозумілі системні повідомлення, музикальні ефекти та інше.

**Як запобігти онлайновому піратству вдома?**

*Шановні користувачі мережі Internet! Не завантажуйте незаконно та не передавайте іншим фільми, музику та програми.*

****** Онлайнове піратство — це незаконне копіювання та розповсюдження матеріалів, що є об'єктами авторського права, для ділового або персонального вжитку.

 Якщо ви займаєтесь піратством цифрових файлів, ви можете піддатися значним штрафам, а ваші комп’ютери, в свою чергу — стати об'єктом вірусів, [шпигунських](http://www.microsoft.com/athome/security/spyware/spywarewhat.mspx) програм та іншого небажаного програмного забезпечення.

Пам’ятайте, що піратство — це та ж крадіжка. Ось декілька прикладів покарання, якому можуть піддати вас, якщо ви незаконно завантажуєте музику чи інші файли:

1. *Згідно з Законом України про авторські права з вас може бути стягнуто штраф. Стаття 512 Кодексу України про адміністративні правопорушення свідчить про накладення штрафу від десяти до двохсот неоподатковуваних мінімумів доходів громадян (170-3400 грн) з конфіскацією незаконно виготовленої продукції та обладнання.*
2. *Ваш домашній комп'ютер та пов'язані з ним файли й диски можуть бути конфісковані.*
3. *Ваш комп'ютер може бути інфікований вірусами та іншими шпигунськими програмами.*

**Використані джерела**

1. Підручник з інформатики для 5 кл. закладів загальної середньої освіти /Н. В. Морзе, В. П. Вембер, О. В. Барна, О. Г. Кузьмінська К: УОВЦ «Оріон», 2018. 256 с.:іл. ISBN 978-617-7485-80-2
2. Інформатика: підруч. для 5 кл. загал. серед. освіти / [О. О. Бондаренко, В. В. Ластовецький, О.П. Пилипчук, Є. А. Шестопалов] – Харків: Вид-во «Ранок», 2018. – 160 с. : іл. ISBN 978-617-09-4781-9
3. Морзе Н.В / Робочий зошит з інформатики: навч. посіб. для 5 кл. загальноосвіт. навч. закл. /Н. В. Морзе,  О.В Барна, В. П.Вембер,О.Г., Кузьмінська. – К.: УОВЦ «Оріон», 2017. – 96 с. – ISBN 987-617-7355-74-7.
4. Learningapps.org [Електронний ресурс] : Інтернет-ресурс для створення інтерактивних вправ – Режим доступу: <https://learningapps.org>

***Турова Р.А., учитель інформатики***

***Синюхинобрідської ЗОШ І-ІІІ ступенів***

**Суд над Інтернетом. Internet: глобальне добро чи зло?**

(позакласний захід для учнів 9-11 класів)

**Дійові особи:** суддя, прокурор, адвокат, Інтернет, свідки звинувачення, свідки захисту, секретар.

**Перебіг заходу**

**Секретар.**Встати! Суд іде!

**Суддя.** Доброго  дня. Прошу  всіх сідати.

Шановні присутні!

На  сьогоднішньому  судовому  засіданні  слухається  позовна  справа

книги проти глобальної мережі Інтернет за  статтями 361, 362 Карного кодексу розділу ХVІ «Злочини у сфері використання електроно-обчислювальних  машин, систем та комп’ютерних мереж» та звинувачення в негативному впливові інтернету на підростаюче покоління. По звинуваченню вестиме судове засідання суддя \_\_\_\_\_\_\_\_\_\_\_\_ при секретарі \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ за участю прокурора\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_адвоката \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. У судовому засіданні беруть участь вчителі інформатики \_\_\_\_\_\_\_\_\_\_\_\_\_.

Пані секретар, оголосіть про явку учасників судового процесу.

**Секретар.** Всі учасники судового процесу присутні в залі та попереджені

про правила поведінки в суді.

**Суддя.** Судове засідання оголошую відкритим!

З’ясуємо особу підсудного. Підсудний, ваше прізвище, ім'я та по батькові?

**Інтернет**. Я – Інтернет – всесвітня система комп'ютерних мереж. Мене також називають мережею мереж. Я складаюся з мільйонів локальних і глобальних, публічних, академічних, ділових і урядових мереж, пов'язаних між собою з використанням різноманітних дротових, оптичних і [бездротових технологій](http://uk.wikipedia.org/wiki/%D0%91%D0%B5%D0%B7%D0%B4%D1%80%D0%BE%D1%82%D0%BE%D0%B2%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0). Я становлю фізичну основу для розміщення величезної кількості інформаційних ресурсів і послуг, таких як взаємопов'язані гіпертекстові документи [Всесвітньої павутини](http://uk.wikipedia.org/wiki/%D0%92%D1%81%D0%B5%D1%81%D0%B2%D1%96%D1%82%D0%BD%D1%8F_%D0%BF%D0%B0%D0%B2%D1%83%D1%82%D0%B8%D0%BD%D0%B0) (World Wide Web — WWW) та [електронна пошта](http://uk.wikipedia.org/wiki/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0_%D0%BF%D0%BE%D1%88%D1%82%D0%B0). Також мене називають «Всесвітня мережа», «Глобальна мережа» чи навіть одне слово «Мережа», «Іне́т», «Тенета», «Міжмережжя», «Інтерне́трі» або «Не́трі».

**Суддя.** Ваш батько?

**Інтернет.** [Джозеф Ліклайдер](http://uk.wikipedia.org/w/index.php?title=%D0%94%D0%B6%D0%BE%D0%B7%D0%B5%D1%84_%D0%9B%D1%96%D0%BA%D0%BB%D0%B0%D0%B9%D0%B4%D0%B5%D1%80&action=edit&redlink=1).

**Суддя.** Ваша  біографія?

**Інтернет.** У [1962](http://uk.wikipedia.org/wiki/1962) році мій батько Джозеф Ліклайдер, вчений в галузі комп’ютерних технологій, керівник Агентства передових оборонних дослідницьких проектів США, висловив ідею Всесвітньої комп'ютерної мережі. У 1969 році Міністерство оборони США започаткувало розробку проекту, котрий мав на меті створення надійної системи передачі інформації на випадок війни. Агентство DARPA запропонувало розробити для цього комп'ютерну мережу. Ця мережа була названа ARPANET (Мережа Агентства передових досліджень).

20 жовтня 1969 року група комп’ютерщиків Каліфорнійського університету вирішила з’єднати свій комп’ютер з комп’ютером Стенфордського дослідницького інституту. Один науковець сидів за комп’ютером у Каліфорнійському університеті, другий у Стенфордському дослідному центрові. Коли відбулося з’єднання, перший мав написати слово **log**, другий – **in.** У результаті утворилося б слово **login**. Але було успішно передано всього дві букви. Проте початок було покладено. Тобто дата мого народження – 20 жовтня 1969.

ARPANET почала активно рости й розвиватись; її дедалі ширше почали використовувати вчені із різних галузей науки. У [1973](http://uk.wikipedia.org/wiki/1973) році до мережі через трансатлантичний кабель були підключені перші іноземні організації з [Великобританії](http://uk.wikipedia.org/wiki/%D0%92%D0%B5%D0%BB%D0%B8%D0%BA%D0%BE%D0%B1%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D1%96%D1%8F) та [Норвегії](http://uk.wikipedia.org/wiki/%D0%9D%D0%BE%D1%80%D0%B2%D0%B5%D0%B3%D1%96%D1%8F) — мережа стала міжнародною. [1 січня](http://uk.wikipedia.org/wiki/1_%D1%81%D1%96%D1%87%D0%BD%D1%8F) [1983](http://uk.wikipedia.org/wiki/1983) року мережа ARPANET перейшла з протоколу [NCP](http://uk.wikipedia.org/w/index.php?title=NCP&action=edit&redlink=1) на протокол [TCP/IP](http://uk.wikipedia.org/wiki/TCP/IP), який досі успішно використовується для об'єднання мереж. Саме у 1983 році за мережею ARPANET закріпився термін «Інтернет».

Історія українського Інтернету починається 19-го грудня 1990 року, коли сектор Юрія Янківського з Міжгалузевого Наукового Центру Технології Програмування «Технософт» (керівник Ігор Вельбицький) під'єднався до світової мережі Інтернет, ставши першим українським абонентом.

**Суддя.** Приступаємо до розгляду судової справи по суті. Пане прокурор, оголосіть, будь ласка, звинувачувальний висновок.

**Прокурор.** Ваша честь, поважна публіка! Упродовж тривалого часу друкована книга була єдиним і основним джерелом інформації. Сьогодні світ заполонили комп’ютери. З комп’ютером «на ти» навіть маленькі діти. Людство жило багато років без інтернету. Навіщо він з’явився на світ? Звичайно, щоб заважати книзі, за неї почали забувати, звузилося коло читачів. Internet посягнув на споконвічне – книги сіяли між людьми зерна мудрості та доброти.

Та це ще не все. Internet обвинувачується в розповсюдженні вірусів і шкідливих програм, а також в пропаганді насильства і жорстокості, в розповсюдженні спаму, порушенні авторських і суміжних прав, спричиненні шкоди етичному і фізичному здоров'ю людини.

**Суддя.** З боку звинувачення були запрошені свідки, які можуть підтвердити перераховані факти?

**Прокурор.** Так ,Ваша честь, дозвольте  викликати  наших свідків.

**Суддя.** Дозволяю викликати для надання свідчень свідків. Суд нагадує про відповідальність за дачу  неправдивих свідчень.

**Секретар.** В зал суду запрошується свідок обвинувачення.

**Прокурор.** Шановний свідок. Поясніть присутнім, яке жахіття трапилося з вашим комп’ютером завдяки інтернету.

**Свідок 1.** Те, що трапилося з моїм комп’ютером, – це жахливо.

Я працював за комп’ютером,  і  він  в  одну хвилину «згас» і більше не запустився. А винен в усьому інтернет.  Адже ним мандрують програми, які потрапивши на комп'ютер чи до локальної мережі, завдають різної шкоди. Особливо небезпечними є два види таких програм — віруси та хробаки. Програмам дали назву біологічних організмів, бо вони досить малі, розповсюджуються, роблячи копії з самих себе, та не можуть існувати без носія. Такий вірус потрапляє до комп'ютерної системи, власник якої про це й гадки не має. До того ж іноді вірус упродовж певного часу жодним чином себе не викриває, і лише після настання певної дати чи події активізується та завдає шкоди комп'ютерній системі.

Хробак схожий на вірус тим, що розмножується, роблячи власні копії, але на відміну від останнього не потребує носія й існує сам по собі. Часто хробаки передаються електронною поштою. Хоча спершу хробаки не були шкідливими, нинішні їхні різновиди спричиняють значні перенавантаження мереж і можуть руйнувати файли. Навіть найменш шкідливі програми з вірусами можуть призвести до великих неприємностей, а завдані ними збитки іноді оцінюють у мільйони доларів. Нині з'являються тисячі вірусів. Якщо 1990-го року їх було приблизно 200-500, то у 2000 році — вже 50 000.

Віруси розповсюджуються по мережі Internet щодня, завдаючи непоправної шкоди ПК і різних незручностей користувачеві. Доводиться обновляти свої антивірусні бази по кілька разів на день, щоб відчути себе в безпеці. Але все таки розробка вірусів шкідлива на рівні безпеки країни, а не тільки окремого користувача.

**Секретар.** В зал суду запрошується член комісії з питань інформаційної політики.

**Прокурор.** Шановний свідку! Що ви можете додати до справи?

**Свідок 2**. Шановний Суд, окрім вірусів, мережею ширяться спами.

Спам (англ. spam) — масова розсилка кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати. Передусім термін «спам» стосується рекламних електронних листів.

Розрізняють такі види спаму:

* Реклама. Цей різновид спаму трапляється найчастіше. Деякі компанії рекламують свої товари чи послуги за допомогою спаму. Вони можуть розсилати його самостійно, але частіше замовляють це тим компаніям (чи особам), які на цьому спеціалізуються. Привабливість такої реклами в її порівняно низькій вартості і досить великому охопленні потенційних клієнтів.
* Нігерійські листи. Іноді спам використовується для того, щоб виманити гроші в одержувача листа. Найпоширеніший спосіб одержав назву «нігерійські листи», тому що дуже багато таких листів приходило з Нігерії. Такий лист містить повідомлення про те, що одержувач листа може одержати якимось чином велику суму грошей, а відправник може йому в цьому допомогти. Потім відправник листа просить перерахувати йому трохи грошей: наприклад, для оформлення документів чи відкриття рахунку. Виманювання цієї суми і є метою шахраїв.

А от боротися зі спамом дуже складно: навіть корпорації, спроможні щорічно витрачати мільйони доларів на антивірусне програмне забезпечення, не здатні зупинити потік рекламних та інших небажаних повідомлень, які призводять до перенавантаження мережних каналів, зайвих витрат дискового простору. Не знають, як його позбутися.

Крім програм, за допомогою яких певні люди намагаються увійти до вашої системи, існують також засоби, що застосовують для спостереження за вами. Це насамперед програмне забезпечення, яке зазвичай називають adware та spyware, шпигунські програми, програми для батьківського контролю, блокувальні програми тощо. Таке програмне забезпечення має багато функцій. Воно може відстежувати ваші звички щодо мандрування Інтернетом, надсилати комусь дані без вашого дозволу, змінювати адресу домашньої сторінки вашого браузера і навіть системні файли комп'ютера.

**Секретар.** В зал суду запрошується представник органів правопорядку.

**Прокурор.** Шановний свідку! Чи правда, що існує категорія людей, яка за допомогою інтернету здійснює атаки на чужі комп'ютери задля отримання персональної інформації?

**Свідок 3.** Так, існує. Зазвичай їхніми об'єктами стають бази даних великих корпорацій, де зберігаються такі відомості, як персональні ідентифікаційні номери, номери банківських рахунків та кредитних карток клієнтів. Проте відомо багато випадків, коли жертвами зловмисників стають приватні особи, особливо якщо вони передають конфіденційну інформацію в інтернеті без належного захисту. Часто зловмисники намагаються викрасти персональну інформацію, для того щоб від імені іншої людини відкривати рахунки, купувати товари тощо. Найчастіше викрадають дані про банківські картки. Анонімність і величезні розміри інтернету роблять їх ласим шматком для шахраїв усіх ґатунків.

Досить часто інтернет стає також джерелом шахрайства та піратства, а ми — потенційними жертвами їх діянь.

5 найпоширеніших способів інтернет-шахрайства:

1. фальшиві товари на аукціонах;
2. банківська афера, або фішинг;
3. афера «Ви виграли безкоштовний Xbox!»;
4. благодійна афера;
5. шантаж.

**Секретар.** В зал суду запрошується психолог.

**Прокурор.** Шановний свідку! Поясніть Суду, яку загрозу несе Internet для психічного і фізичного здоров'я людей.

**Свідок 4.** Найпоширенішою формою інтернет-залежності є спілкування по інтернету. Це небезпечно тим, що людина поступово розучується спілкуватися в реальному житті, у спілкуванні по інтернету можна відчути себе героєм, який може все або багато з того, що забороняється йому в реальному світі. Тут можна самостійно ухвалювати рішення і не боятися відповідальності. Школярі часто йдуть у комп`ютерний світ у пошуках свободи і самоствердження.

Багато людей почали використовувати всесвітню мережу не тільки для роботи чи пошуку інформації, а як засіб життя. З’явилися *чати, сайти знайомств*. Люди днями і ночами листуються, бавляться в ігри, користуються відео-чатами. Відповідно до нових діагностичних рекомендацій, інтернет-залежною визнається людина, яка проводить в мережі не менше шести годин на день і у якої спостерігається щонайменше один із симптомів залежності протягом попередніх трьох місяців. За статистикою, 54% користувачів у віці від 13 до 23 років проводять в інтернеті щоденно від 1 до 3 годин, ще 31% — по 4-6 годин. Існує категорія людей, яка живе віртуальним життям по 10 годин на добу і більше. Більше 45% всіх опитаних заявили, що без персонального комп’ютера і підключення до інтернету вони не змогли б жити. Це більше, ніж для будь-якого іншого медіапристрою (28% молодих людей не можуть жити без мобільного телефона, 11% — без телевізора).

Важкою формою інтернет-залежності є геймерство. Це обумовлено відсутністю необхідності в яких-небудь навичках роботи з персональним комп’ютером.

До симптомів інтернет-залежності відносять:

1) нав’язливе бажання підключитися до інтернету;

2) хвороблива нездатність вчасно відключитися від інтернету;

3) розумове або фізичне виснаження;

4) порушення сну або концентрації уваги;

5) дратівливість, депресія, труднощі у спілкуванні з людьми в реальному житті.

З’ясовуючи вплив інтернету на організм людини, науковці академії наук в Китаї провели високоточне дослідження, магнітно-резонансну томографію, і довели, що інтернет-залежність згубно впливає на мозок людини. Як зазначають дослідники, вплив цього виду залежності на організм людини (а особливо на головний мозок) є майже ідентичним, дуже подібним до впливу, який на собі відчувають наркозалежні та алкоголіки.

**Секретар.** В зал суду запрошується свідок, інтернет-залежний користувач.

**Прокурор.** Шановний свідку! Як вплинув інтернет на Ваше життя?

**Свідок 5.** Я усвідомлюю, що хворий. Я приходжу додому з школи — і відразу включаю комп’ютер і заходжу в Internet. Мені фізично погано, якщо немає доступу до мережі… Я провожу там весь свій час, я не ходжу на вулицю, не спілкуюся з друзями... Я не сплю ночами, не роблю уроки… Мої типи мережевих захоплень:

* нав’язливий серфінг — пошук інформації, подорожі по мережі;
* віртуальне спілкування — листування, участь в чатах, форумах, поява багатьох віртуальних знайомих;
* віртуальний шопінг — мережеві азартні ігри, аукціони, непотрібні покупки в інтернеті;
* ігрова залежність — комп’ютерні і мережеві ігри.

І у всьому цьому винуватий Internet! Я практично втрачений для суспільства, але нічого не можу з цим поробити!

**Суддя.** Слово для захисту надається адвокату.

**Адвокат.**  Шановні присутні, я хочу вам нагадати, що основне призначення Internet — це отримання необхідної інформації в максимальному об’ємі за мінімальну кількість часу. Будь-яка протидія використовуванню Internet сучасним людством є кроком назад в історичному розвитку. Internet дає людям свободу. Він повинен існувати і не бути чиєюсь власністю. Ми теж запросили свідків, яким є що сказати про плюси Internet.

**Секретар.** В зал суду запрошується свідок захисту.

**Адвокат.** Шановний свідку! Чи правда, що Internet серйозно зарекомендував себе як найкраще джерело інформації.

**Свідок 1.** Так, це абсолютна правда. За допомогою Internet можна дістати доступ до навчальних програм, до системи дистанційної освіти, особливо цікаво вивчати мистецтво, використовуючи сайти різних музеїв. Ви зможете подорожувати по залах Ермітажу, не виходячи з будинку і не штовхаючись в натовпі туристів. Ви зможете потрапити в Білий дім у Вашингтоні, познайомитися з сім’єю американського президента.

В школах інтернет використовують для навчання. Це і презентації на уроках, і відеоуроки по проведенню хімічних реакцій і фізичних експериментів, і використання комп’ютерів для математичного моделювання тощо. Але наука не стоїть на місці — і те, що використовувалося сьогодні, вже може бути неактуальне завтра. І, здається, це головна мета використовування Internet в школі — отримання свіжої інформації і оновлення програмних продуктів для нашого подальшого навчання.

У наш час найпопулярнішими службами Інтернету є:

* вебфоруми;
* блоги;
* вікіпроекти (в  тому  числі  й  Вікіпедія);
* інтернет-магазини;
* інтернет-аукціони;
* інтернет-події;
* інтернет-час;
* електронна пошта;
* групи новин;
* файлообмінні мережі;
* електронні платіжні системи;
* інтернет-радіо;
* інтернет-телебачення;
* ІР-телефонія;
* системи обміну повідомленнями.

Для багатьох людей інтернет — спосіб заробітку.

**Секретар**. Для надання свідчень в зал суду запрошується свідок – користувач-школяр.

**Адвокат.** Шановний свідку! Що нового в освіті пропонує Internet?

**Свідок 2.** Те, що з десяток років тому було сюжетом для фантастичних оповідань, тепер стає в школі реальністю. Дистанційне навчання, доступ до величезного архіву інформації з будь-якого предмета, можливість використання відео, аудіо та інших медіа-матеріалів — це привіт зі світу фантастики. У всьому світі школи переходять на такий спосіб навчання не тому, що їх до цього примушують, а тому, що це зручно для всіх учасників навчання!

Школярі мають можливість спілкуватися з учителями на інтернет-форумах, а вчителі в електронному вигляді можуть давати завдання конкретному учневі і дивитись, у який термін і наскільки успішно ці завдання виконуються.

**Секретар**. До залу суду запрошується представник ІТ-компанії.

**Адвокат.** Шановний свідку, що ви можете повідомити на захист інтернету?

**Свідок 3.** Кожен користувач інтернету повинен знати «Правила безпечної роботи в  інтернеті».

**1.** Захистіть свій комп'ютер! Регулярно оновлюйте операційну систему, використовуйте антивірусну програму, використовуйте брандмауер. Створюйте резервні копії важливих файлів. Будьте обережні, завантажуючи файли з інтернету.

**2.** Розповідайте батькам та дорослим про нові можливості, знайдені вами під час роботи в інтернеті. Насолоджуйтеся інтернетом разом з ними.

**3.** Зберігайте свої паролі в таємниці. Вони повинні бути простими, але такими, що їх складно вгадати. Дата народження не доречна як пароль.

**4.** Довіряйте своїй інтуїції. Якщо щось в онлайні примушує вас нервувати, поговоріть про це з дорослими.

**5.** Виберіть правильно ім'я користувача й перевірте, щоб воно не відображало жодної особистої інформації про вас.

**6.** Ніколи не давайте своєї адреси, номера телефону або іншої персональної інформації, включаючи інформацію про те, яку школу ви відвідуєте або де вам подобається гратися чи відпочивати.

**7.** Поводьтеся чемно і ніколи не ображайте інших. Правил культурної поведінки треба дотримувати не тільки в реальному житті, але й тоді, коли знаходитеся за комп'ютером.

**8.** Поважайте чужу власність в онлайні. Створення незаконних копій творів інших людей: музики, відеоігор, програм — це все одно, що крадіжка товару в магазині.

**9.** Ніколи не зустрічайтеся зі своїми онлайн-друзями особисто. Вони можуть бути не тими, за кого себе видають.

**10.** Пам'ятайте: не все, що ви читаєте або бачите в онлайні, є правдивим. Запитайте в дорослих про те, в чому ви невпевнені.

 Якщо ми буде дотримуватися цих правил, то в інтернеті почуватимемо себе цілком безпечно. Не треба боятися і вірусів. Проти них існує безліч антивірусних програм: Доктор Веб, Аваст, Касперський, Нортон-Антивірус та багато інших. Лише треба вчасно оновлювати їх, щоб вони змогли боротися з новоствореними вірусами. А на спам, який надійшов на ваш комп'ютер, просто не треба відповідати.

**Суддя:** Обвинувачений, ваше останнє слово!

**Інтернет.** Я не визнаю свою провину. Я — лише ресурс, який надає певні можливості. А як мене використовуватимуть — для користі або на шкоду — залежить від конкретних людей. Отже, судити треба не мене, а користувачів, які використовують мої ресурси для протизаконних дій! На свій захист я хочу навести деякі статистичні данні.

Понад 4 мільярди користувачів інтернету було зафіксовано по всьому світу в 2018 році. Практично половина з них — жителі азіатських країн 44%, в Європі — близько 23%, на Північну Америку припадає близько 13% користувачів мережі, а кожен десятий користувач з Латинської Америки. На Африку, Близький Схід і Австралію відповідно 6%, 3% і 1% користувачів. Майже половина всіх інтернет-користувачів світу молодші 25 років. Лідером за кількістю інтернет-користувачів серед окремих країн є Китай, де мережею користуються понад 485 млн. осіб, при тому що рівень проникнення інтернету складає лише 36%. Кількість вебсайтів в інтернеті складає більш як 1 мільярд.

Серед соціальних мереж лідером за кількістю користувачів залишається Facebook. Мобільна аудиторія Facebook, за оцінками The Royal Pingdom, складає 470 мільйонів. Кількість зареєстрованих акаунтів на Twitter — 325 мільйонів, а в день всі користувачі сервісу відправляють близько 450 мільйонів твітів.

Інтернет — це воістину грандіозне місце! Кількість даних, які люди створюють, діляться і споживають в інтернеті практично неможливо уявити у фізичному форматі.

Тим не менш, скільки ж даних насправді розкидано по всесвітній мережі? Що ж відбувається за один день в інтернеті?

1. За один день інтернет-трафіком споживається така кількість інформації, щоб заповнити 168 000 000 дисків DVD.

2. Надсилається 294000000000 листів, і знадобилося б два роки, щоб обробити таку кількість справжніх листів.

3. З’являється близько 2 мільйонів постів у блогах. Цього достатньо, щоб заповнити відомий журнал Time на 770 років вперед.

4. 172 000 000 різних людей відвідують Facebook.

5. 40 мільйонів людей відвідують Twitter.6. 20000000 відвідують [Google](http://www.webochka.com/component/content/article/1-golovna/395--google.html)+.

7. Близько 4,7 мільярдів хвилин люди проводять на Facebook. Вони оновлюють 532000000 статусів. Завантажують 250 000 000 фотографій. Якби довелося все це роздрукувати, то ця купа фотографій заповнила б 80 Ейфелевих веж.

8. 846 000 годин відео завантажується на Youtube. Це близько 98 років безперервних зйомок відео.

9. Більш 1288 нових додатків з’являється для скачування і більше 35 мільйонів додатків скачується.

**Суддя.** Заслухавши свідків і останнє слово звинуваченого, переходимо до дебатів. Слово надається прокурору.

**Прокурор.** Шановний  суд! Всі присутні. Я хочу звернути Вашу увагу на те, що інформаційному полю України притаманна гіпердевіація (агресія, цинізм, цінності кримінального світу тощо), що призводить до формування асоціальної поведінки дітей і молоді. Аналіз підтверджує, що найбільш схильними до негативного впливу сучасного інформаційного простору є підлітки, які ще не навчилися оцінювати отримані відомості. Сьогодні кожний, хто користується інтернетом, може знайти документальні фото, відео вбивств, зґвалтувань, побиття, катувань, інших форм насильств, що породжують страх. Завдяки різним видам комунікації у віртуальному середовищі має місце кримінальна експлуатація дітей. За даними ООН, в 79% торгівля людьми здійснюється з метою сексуальної експлуатації. За даними ЮНІСЕФ, кожного року 1,2 мільйона дітей потрапляють до тенет торгівлі людьми з метою сексуальної експлуатації та примусової праці.

Таке явище як «комп’ютерна залежність» формується набагато швидше, ніж будь-яка традиційна залежність: куріння, наркотики, алкоголь. Аналіз підтверджує, що у середньому потрібно не більш півроку, щоб стати комп’ютерним адиктом (залежною людиною). Згідно з даними різноманітних досліджень, сьогодні інтернет-залежними є близько 10 % користувачів у всьому світі. Крайнім ступенем негативних наслідків інтернет-залежності є перетворення людини (в першу чергу, підлітка) в «інтернет-мауглі». Люди з синдромом мауглі – це така категорія людей, які в силу тривалого перебування в кіберпросторі втрачають зв’язок з реальністю, інколи навіть не здатні розрізнити віртуальний та реальний світ, втрачають мовні навички, при спілкуванні з оточенням займають по відношенню до нього ворожу, агресивно-негативну позицію. Як правило, в повсякденному житті вони мляві, апатичні, сумні, пасивні, позбавлені життєрадісності, у них знижена пізнавальна активність, вони нездатні до конструктивного виходу із конфліктної ситуації. Процес негативного впливу інтернет-середовища на свідомість людини може призвести до трагічних наслідків як для здоров’я, так і для суспільства. Отож вина інтернету повністю доведена.

**Суддя.**  Слово надається адвокатові.

**Адвокат.** Шановні присутні. Я вважаю що переваг в інтернету  більше, ніж  недоліків:

* інтернет – безцінне сховище людського досвіду і корисної інформації. Будь-хто охочий може використовувати його вміст для своїх цілей;
* інтернет – необмежене спілкування, що включає в себе листування, голосове спілкування, відеозв’язок. У соціальних мережах можна знайти своїх однокласників, однокурсників, товаришів по службі, колег;
* інтернет – місце, де можна висловитися, проконсультуватися, поділитися з людьми досвідом;
* створювати сайти в інтернеті останнім часом стало неймовірно просто – всього кілька кліків і добротний сайт готовий;
* в інтернеті можна завантажувати ігри, фотографії, мелодії, пісні, відео, документи;
* в інтернеті завжди можна знайти однодумців або просто веселу компанію;
* інтернет робить людину більш освіченою, розсудливою – багатьом речам можна навчитися, не відходячи від монітора;
* в інтернеті можна заробляти. Письменник, дизайнер, програміст і багато інших зможуть знайти в інтернеті хороший стабільний заробіток;
* в інтернеті можна відчувати себе вільніше, ніж в реальному світі;
* в інтернеті можна широко самореалізуватися;
* в інтернеті можна стежити за останніми новинами в світі і в своїй країні;
* в інтернеті можна рекламувати свою корпорацію, займатися бізнесом, брати участь в торгах, аукціонах, грати на біржах.

Щодо бібліотеки. Вона завжди була й надалі збережеться як інтелектуальний та інформаційний центр.

**Суддя.** Чи не хоче хтось із засідателів висловити свою думку з приводу справи, що розглядається?

**Слово вчителя.** Протягом судового засідання нам вдалося поглянути на глобальну комп’ютерну мережу Internet з різних сторін. Виявлені як позитивні, так і негативні її якості. Хотілося б сказати словами одного з великих сучасників:«Інтернет, він не зближує. Це скупчення самотності. Ми начебто разом, але кожен один. Ілюзія спілкування, ілюзія дружби, ілюзія життя».

Тож поки маєте можливість не промінюйте реальне спілкування з близькими і друзями на віртуал. Колись цього може так не вистачати. І жодна мережа ніколи вам не компенсує цього спілкування.

**Суддя.** Суд, розглянувши всі обставини справи і вислухавши всіх свідків, вирішив:

Internet — двозначна річ. З одного боку, це простір свободи й прозорості, з іншого — контролю. Internet увібрав в себе не тільки достоїнства глобальності, але і глобальні вади. Технічний прогрес зупинити неможливо, але слід пам’ятати, що у будь-якої новини є свої позитивні і негативні сторони. І чим стане Internet в нашому житті, залежить від людини… Вирок остаточний і не оскаржує! Судове засідання оголошується закритим!

**Використані джерела**

1. Безпека дітей в Інтернеті: корисні інтернет-посилання на інформацію та відео про грумінг, секстинг, кібербулінг [Електронний ресурс]. – Режим доступу: <http://cynkalovskyi.school.org.ua/news/11-28-29-08-04-2019/>
2. Сидоренко О.О. Рольова гра «Суд над Інтернетом. Internet: глобальне добро або зло?» – [Електронний ресурс]. – Режим доступу: <https://vseosvita.ua/library/rolova-gra-sud-nad-internetom-internet-globalne-dobro-abo-zlo-101792.html>

***Кулачинська Т.В., учитель інформатики***

***Кумарівської ЗОШ І-ІІІ ступенів***

**Подорож океаном Інтернету**

(позакласний захід для учнів 5-6 класів)

**Мета:** створити умови для засвоєння учнями знань з інформаційної безпеки, сформувати правила роботи в мережі Інтернет та зниження її негативного впливу; сприяти розвитку інформаційно-комунікаційної культури та грамотності учнів як фактора безпеки в інформаційному суспільстві,формуванню пізнавальної, інформаційної та комунікативної компетентностей;виховувати почуття взаєморозуміння, дружби, розвивати творчу активність.

**Форма проведення:** змагання.

**Обладнання:** картки із завданнями, аркуші паперу формату А4, грамоти.

**Перебіг заходу**

**Ведучий 1.**

Минають дні, минають роки.

Прогрес крокує повсякчас,

І вже досягнення науки

Прийшли до школи і до нас.

Тож не барімося, до діла,

Ми зараз конкурс проведем,

Та інтернет-знавців умілих

Сьогодні тут ми віднайдем.

**Ведучий 2.** Тож розпочинаємо конкурс знавців інтернету. Сьогодні я вас запрошую у подорож, але не просту, а казкову – подорож океаном всесвітньої мережі.

**Ведучий 1**. Перш за все познайомимося з учасниками конкурсу, тобто командами. Для цієї подорожі оберіть капітанів та придумайте командам назву своїх кораблів. (*Представлення команд*).

**Ведучий 2**. Та яке змагання без журі? Оцінити ваші вміння, знання люб'язно погодилися…

(*оголошує членів журі*)

**Ведучий 1.** Команди познайомилися одна з одною. Отже, можна розпочинати нашу подорож. А починається вона з **острова «Розминки»**.

Мешканці острова просять розібратися з запитаннями, яким вони не можуть дати раду. А ви, сподіваємося, допоможете їм в цьому. Кожна правильна відповідь буде оцінюватися не просто балами, а віртуальними грошима – бітерами. Яка команда заробить більше, та й перемогла. А віртуальні кошти вам допоможуть здійснити наступні подорожі.

**Ведучий 1.** Запитання для першої команди:

1. Комп’ютери, з’єднані між собою. (*Мережа*)
2. Програма для спілкування. (*Чат*)
3. Електронна «книжка», де міститься різна інформація. (*Сайт*)
4. Як називають сторінки сайту? (*Вебсторінки)*
5. Як називаються програми для роботи з Інтернетом? (*Браузери*)
6. Особа, яка зламує та проникає у системи даних, не маючи на це дозволу. (*Хакер*)
7. Програма, яка знаходить і знищує віруси. (*Антивірусна програма*)
8. Програма, що саморозмножується, поширюється з файла на файл і з комп’ютера на комп’ютер. (*Вірус*)
9. Як називають повідомлення, яке надходить до одержувача майже миттєво після його надсилання? (*Миттєве повідомлення*)
10. Як називається область даних на диску, що має ім'я? *(Файл)*

**Ведучий 2.** Запитання для другої команди:

1. Служба, призначена для обміну повідомленнями через електронні поштові скриньки. (*Електронна пошта*)
2. Як називається вчинок, коли чужі матеріали видають за власні? (*Плагіат*)
3. Назвіть пристрій введення інформації, розташований на вашому робочому місці. *(Клавіатура)*
4. Що об’єднує сайти Yahoo, Google, Мета? (*Пошукові системи*)
5. Всесвітня система об’єднаних комп’ютерних мереж, побудована на використанні протоколу IP. (*Інтернет*)
6. Програма, що саморозмножується та існує без носія. (*Хробак*)
7. Як називається поштова кореспонденція в основному рекламного характеру, що приходить на e-mail адресу користувача без його запиту? (*Спам)*
8. Американська фірма, яка є лідером з виробництва комп'ютерного програмного забезпечення. (*Майкрософт*)
9. Назвіть пристрій введення інформації, розташований на вашому робочому місці. *(Клавіатура)*
10. Мережевий щоденник, який користувачі можуть час від часу наповнювати текстом та мультимедійними даними. (*Блог*)

***(Результати 1 конкурсу)***

**Ведучий 2.** Антична мудрість говорить: «Знання – це сила». Ви показали наскільки ви сильні знаннями. Що ж, відвідини першого острова допомогли заробити перші бітери. Доведеться добре попрацювати й надалі, щоб їх було більше, ніж у команди суперника.

**Ведучий 1.** Подорож продовжується. Зараз ми заходимо в **порт «Ерудит»**. Для того, щоб мати враження про вас, мешканці підготували своє завдання: з поданих слів за 1 хвилину скласти кросворд. Чим більше перетинів у вашому кросворді – тим більше отримаєте (3 бітери).

Слова для кросворду: *клавіатура, модем, сайт, байт, блог, вінчестер, гігабайт, біт, сканер, процесор, форматування, інформатика, мережа, гіперпосилання, завантаження, Інтернет.*

***(Результати 2 конкурсу)***

**Ведучий 2.**  Наш корабель пройшов ще одне нелегке випробування.

По курсу **острів «Казковий»**. Відвідувачів цього острова зустрічає Шахерезада і розповідає свою загадкову історію. Ось і сьогодні вона для вас підготувала незвичайну казку *– «Казка про Скріпочку»*. Уважно її слухайте, адже після цього Шахерезада дасть вам наступне завдання для виконання.

*(На початку гри кожному з учасників видається канцелярська скріпка (бажано, кольорова).*

**«Казка про Скріпочку»**

**Шахерезада**. Я пропоную до вашої уваги казку про дівчинку Скріпочку, таку ж, як і у вас в руках. Скріпочка була дуже товариська і весела. На день народження батьки подарували їй комп’ютер та підключили до мережі Інтернет, тепер у неї з’явилося більше можливостей для спілкування.

*(Учасникам пропонується розігнути скріпочку і зробити з неї усмішку).*

Спілкуючись в «Інстаграмі» з друзями, одного разу вона отримала цікаве повідомлення від незнайомого хлопця, який незабаром запропонував їй дружбу. З кожним днем спілкування Скріпочка розуміла, що в них багато спільного, та й за віком хлопець був лише на один рік старший за неї. На фото, яке вона отримала, він був дивовижно гарним і добрим, тому у Скріпочки не виникло сумнівів щодо зустрічі з ним. Але говорите про це батькам дівчинка не стала, адже думала, що повернеться додому раніше, ніж вони прийдуть з роботи.

Скріпочка уявляла, що її новий друг прийде на зустріч з гарними квітами.

*(Учасникам пропонується зробити зі скріпочки квітку)*

Коли ж дівчинка прийшла на призначене місце зустрічі, там було темно і безлюдно, проте це її зовсім не турбувало, адже її новий знайомий хотів, щоб їм ніхто не заважав. Пройшов деякий час, і раптом перед Скріпочкою з’явився неохайно вдягнений дорослий чоловік. Як з’ясувалося – це був той, хто видавав себе в інтернеті за чемного і доброго хлопця.

Чоловік відібрав сумку і мобільний телефон та почав погрожувати, якщо Скріпочка розповість про нього. Дівчинка дуже злякалась, вирвалась з рук чоловіка та побігла додому. Ця історія дуже вразила Скріпочку. Вона хотіла забути про те, що сталося і повернути все на свої місця.

*(Учасникам пропонується повернути скріпочку в первину форму)*

- У вас вийшло? Ось і у Скріпочки не вийшло.

- Як ви гадаєте, де допустила помилку Скріпочка?

- Що було необхідно зробити інакше?

*(Учасники відповідають на поставлені запитання)*

**Шахерезада.**  ПАМ’ЯТАЙТЕ:

Якщо хтось незнайомий запропонує вам дружбу в Інтернеті, згадайте казку про маленьку Скріпочку та дотримайтесь цих правил:

* не вірте тим даним і фотографіям, які вам надсилають;
* погоджуйтеся на зустріч лише вдень та в людному місці;
* повідомте батькам про зустріч або візьміть їх з собою.

**Шахерезада**. А тепер моє завдання: пропоную вам визначити безпечний чи небезпечний інтернет. Перша команда називає *позитивні сторони* інтернету, а друга – *негативні*. Команди говорять по черзі. За кожну правильну відповідь – 1 бітер.

***(Результати 3 конкурсу)***

**Ведучий 1.** Дякуємо командам за таку чудову подорож. Вже половина шляху позаду, настав час пришвартуватися для невеличкого відпочинку. А це ви зможете зробити на **причалі«Дозвілля»**, погравши в ***гру «Віруси».***

**Ведучий 2.**  Шановні учасники, спробуймо відчути на собі вірусну атаку і постараймося захиститися від неї. Правила будуть такі: вам потрібно з листочків паперу чорного і білого кольорів зробити кульки. Кожен повинен зробити по 2 кульки білого і чорного кольорів. Чорні кульки – «небезпечні», а білі – «безпечні». За моєю командою починаємо кидати один в одного кульками. Задача однієї команди – якнайшвидше закидати протилежну команду «небезпечними» кульками, а «безпечні» залишити на своїй території.

**Ведучий 1.** Кожна біла кулька, яка опиниться на полі команди принесе їй 1 бітер, а чорна – навпаки забере 1 бітер. Час пішов. Починаємо!

***(Результати 4 конкурсу)***

**Ведучий 2.** Наша подорож триває. Погода псується, туман заважає рухатися, а попереду небезпечна ділянка – **мис «Туманний»**. А щоб його обминути, необхідно розшифрувати хмари слів.

**Ведучий 1.** Кожна команда отримує хмару слів, в якій заховане правило безпеки в інтернеті. Та команда, яка впорається швидше, отримає 5 бітерів.

***Завдання для першої команди.***

*(*Відповідь: *Не можна повідомляти своє прізвище, ім’я, домашню адресу, номер мобільного телефону, школи, клас, логіни, паролі.)*

***Завдання для другої команди.***

*(*Відповідь: *Не відкривайте електронні листи від незнайомих адресатів або тих, кому не довіряєш)*

***(Результати 5 конкурсу)***

**Ведучий 1.** Дякуємо командам, що вони вправно подолали всі перешкоди та обминули мис «Туманний» і тепер ми наближаємося до ***острова «Загадковий»****.*

**Ведучий 2.** Мешканці острова вам підготували загадки. Відгадаєте, зможете рухатися далі, а ні – залишитеся на цьому острові назавжди.

**Ведучий 1.** Кожна команда отримає опис загадкової програми. Вам необхідно відгадати про що йде мова та дати відповідь на питання. За правильні відповіді ви отримаєте по 2 бітери.

Загадка для першої команди

Це різновид комп’ютерної програми, особливістю якої є здатність до самостійного розмноження. Потрапляючи в комп’ютер, вона може створювати свої копії, поширюватися, з’єднуватися з іншими програмами або замінювати їх. Також може призвести до псування або видалення інформації, передачі конфіденційних або персональних даних зловмисникам по мережі Інтернет. Вона може маскуватися під нешкідливі вкладення: картинки, документи, посилання на інші сайти тощо.

* Яку назву має загадкова програма?
* Визначте безпечне правило для цього випадку.

(Відповідь: *вірус.*Правило безпеки:*Не відкривайте листи з цікавими заголовками від невідомих відправників. Встановлюйте антивірусні програми. Звертайтеся за допомогою до батьків і вчителів.)*

Загадка для другої команди

Це програмне забезпечення для комп'ютера або іншого електронного пристрою, як правило, під'єднаного до інтернету, що дає можливість користувачеві взаємодіяти з текстом, малюнками або іншою інформацією на гіпертекстовій вебсторінці.

* Яку назву має загадкова програма?
* Знайдіть безпечне правило для цього випадку.

(Відповідь: *браузер.*Правило безпеки:*Не заходити на сайти, які браузер визначає як небезпечні)*

***(Результати 6 конкурсу)***

**Ведучий 1.** Обережно, праворуч від кораблів мілина. Щоб не сісти на неї, треба обов'язково пройти ***«Реставрацію»***. Кожну команду очолює капітан. Перевіримо їх логічне мислення. Завдання капітанам – з окремих слів скласти певні вислови. Хто швидше і правильно це виконає – отримає 2 бітери.

*Вислів для капітана 1 команди*. Не вплутуйтесь в конфлікти з користувачами інтернету і не допускайте їх.

*Вислів для капітана 2 команди*. Дотримуйтесь тих самих стандартів поведінки, що й у реальному житті.

***(Результати 7 конкурсу)***

**Ведучий 1.** Хочу привітати вас з бездоганним подоланням усіх труднощів, які приготував сьогодні океан Інтернету. І оскільки ми з вами покинули останній острів, то тепер нас чекає плавання по безкрайому океану комп'ютерних знань. Деякі учасники мали змогу отримати певні кошти, які знадобляться в наступних подорожах. А яка команда виграла, нам скаже шановне журі.

***(Оголошення результатів. Нагородження переможців і учасників)***

**Ведучий 2.** На жаль, гра закінчилася. Та ми побували на багатьох островах, дізналися багато нового та, звичайно ж, поповнили свої знання.

На завершення нашої зустрічі пропоную послухати вірш про інтернет.

Не можу уявити життя без Інтернету,

Що всі куточки світу заплів в свої тенета.

Лиш кнопку я натисну – відкриються в вікні

Новин велика збірка, і правила, й статті.

Встають переді мною найвищі в світі гори,

Ліси стоять стіною, хлюпочуть хвилі моря.

Я побуваю в шахті і в космос піднімуся.

З подругою в «Інстаграмі» я легко поділюся.

Та є у «павутинні» картинки нехороші,

І сайти підозрілі, настроєні вороже.

Учись добру в мережі, шукай знання й новини,

А сайти злі, що брешуть, обходить ти повинен.

**Вчитель.** Суспільство розвивається швидкими темпами. Інтернет уже зараз став невід’ємною його частиною і сприяє блискавичному руху вперед. Цілком ймовірно, що у найближчому майбутньому Всесвітня мережа повністю замінить усі інші засоби зв’язку. Та зупинімося на мить і замислимось, чи дійсно ми хочемо провести усе життя у віртуальному світі? Бачити аватарки замість живих облич, смайлики замість живих усмішок? На що втрачати власний час – це вільний вибір кожного.

Але, діти, пам’ятайте, що інтернет – це лише інструмент, яким ви користуєтесь, щоб отримати відповіді на свої питання, підготувати реферати та доповіді, спілкуєтесь, якщо між вами величезні відстані. Вчіться користуватись інтернетом із розумом!

До нових зустрічей!

**Використані джерела**

1. Діти в Інтернеті: як навчити безпеці у віртуальному світі: посібник для батьків / І. Литовченко, С. Максименко, С Болтівець [та ін.]. – К.: ТОВ «Видавничий будинок «Аванпост-Прим»», 2010. – 48 с.
2. Виховання культури користувача Інтернету. Безпека у всесвітній мережі: навчально-методичний посібник / А. Кочарян, Н. Гущина. – К., 2011. – 100 с.
3. Безпечне користування сучасними інформаційно-комунікативними технологіями / О. Удалова, О. Швед, О. Кузнєцова [та ін.]. – К.: Україна, 2010. – 72 с.

***Крохмальна О.А., вчитель інформатики***

***Лукашівського НВК***

***Тема:*** «Подорож у світ Інтернету, або як Незнайко заплутався у всесвітній павутині»

***Мета:***

* ознайомити учнів з позитивним та негативним впливом Інтернету на людину;
* дати можливість учням самостійно прийняти ту позицію, до якої вони схиляються;
* дослідити позитивні і негативні сторони інтернету;
* засвоїти правила безпечної роботи в інтернеті;
* розвивати логіку, кмітливість;
* сприяти обізнаності учнів про небезпеки, які існують в інтернеті й соціальних мережах та про шляхи їх подолання, розвитку самооцінки та самоаналізу;
* виховувати інтерес до порушеної теми, інформаційну культуру учнів, етичне спілкування.

***Форма проведення:*** практичне заняття з елементами рольової гри та тренінгу.

***Обладнання:***відео, стікери, значки вірусів і антивірусів, фломастери, комп'ютерна презентація, ватман, музичний супровід, шапка Незнайка.

*Інтернет – це диво-звір!*

*Його можливостям не вір:*

*То цікавий, то небезпечний –*

*Будь з ним ти дуже обережний.*

**Перебіг заходу**

1. **Вступне слово**

**Доброго дня! Сьогодні в нас з вами незвичайна зустріч. Ми будемо подорожувати стежками цікавого світу, назву якого вам слід відгадати.

Це цікавий та захоплюючий світ, який дозволяє вам дізнаватись про все цікаве, спілкуватись з людьми в різних кінцях світу, не виходячи з власного будинку, грати в цікаві ігри та ділитись з іншими своїми думками та захопленнями. Сучасна людина не уявляє собі життя, не побувавши там. То що ж це за світ? *(Відповіді дітей)*

Правильно, це світ інтернету. *(На дошку кріпиться назва «Світ Інтернету»)*

Сьогодні, 5 лютого 2019 року, у світі відзначається День безпечного Інтернету під гаслом «Разом для найкращого Інтернету».

Ми живемо в епоху інформаційних технологій, які увійшли у життя кожного з нас. Ніхто не заперечуватиме, що тепер інтернет відіграє важливу роль у житті людей. Просто вражає, скільки часу у нас забирає інтернет. З уроків інформатики ми знаємо, що цей світ не лише дуже цікавий, а ще й підступний та небезпечний. А вирушаємо ми в подорож для того, щоб віднайти позитивні та негативні сторони інтернету. Тому, щоб туди потрапити, нам потрібна ґрунтовна підготовка і допомога.

Сьогодні я запросила до нас для підтримки нашого вірного друга – Незнайку. Тільки він десь затримується. Тож поки його немає, пропоную об’єднати наші знання про інтернет.

1. **Вправа «Позитивні та негативні сторони інтернету»**

Інтернет – дуже потужний ресурс, який значно полегшує життя людини та відкриває майже необмежені можливості для самореалізації та саморозвитку юної особистості, спілкування, навчання, дозвілля. Але разом з тим в інтернеті приховано досить багато небезпек як для дітей, так і для дорослих. Знання цих небезпек дозволить їх уникнути. Оголошую голосування «За і проти».

*(Учні називають позитивні і негативні можливості інтернету, роблять записи на плакаті)*

Без комп’ютерів цивілізоване суспільство не можна вважати повноцінним, застосування комп’ютерів поширюється кожного дня і буде поширюватися у майбутньому. Як слід користуватися комп’ютером так, щоб можна було зберігати фізичне, психічне та духовне здоров’я. Та перед нашою подорожжю запам’ятаймо кілька правил:

* *Бути позитивним, активним.*
* *Говорити те, що думаєш.*
* *Говорити коротко.*
* *Не перебивати.*
* *Говорити тільки за темою.*
* *Стежити за часом.*
* *Не критикувати, бути толерантним.*

1. **Вправа «Хто надіслав тобі листа?»**

*(На екрані з’являється слайд презентації з зображенням вхідних листів)*

* Чи знайоме вам слово «Нік»?

*Відповідь: «Нік» – це вигадане ім’я, прізвисько, яке вживають користувачі інтернет-форумів, не називаючи своє справжнє ім’я.*

* Навіщо потрібен Нік?
* Що може приховувати Нік?

*Учням роздають стікери та фломастери.*

* Ваше завдання написати листа з привітанням і побажанням другові, не називаючи його імені, та підписати свій лист вигаданим Ніком знизу стікера. Після цього прикріпити стікер на дошці.

*Після того, як всі учні прикріпили листи, учні беруть будь-який стікер з дошки, окрім свого, зачитують листа і намагаються відгадати, хто його написав.*

* Так само відбувається і зі спілкуванням в інтернет-просторі. Дуже складно перевірити, хто саме пише тобі листи, спілкується з тобою. Але в Інтернет просторі ти ніколи не знаєш, хто знаходиться по той бік комп'ютера або мобільного телефону.

1. **Практичне завдання.**

***Розв'язування ситуаційних задач, поданих у листах.***

*Всім привіт!*

*Нещодавно зареєструвався на форумі «Знайомство з Інтернетом» і ось тепер немає мені спокою. Листи надходять один за одним, а в мене не вистачає часу на те, щоб на них відповісти, та й, якщо чесно, і не знаю, як правильно вчинити в описаних ситуаціях. Якщо допоможете розібратись, то доберусь до вас швидше.*

*Буду... через пару рівнів, ой через пару хвилин.*

*Ваш друг Незнайко.*

* Привіт, я, учениця 4-го класу Софія Мережна, зайшла на незнайомий сайт. Раптом на екрані комп'ютера з'явилися незрозумілі повідомлення. Що мені робити?

А) Закрити сайт

Б) Звернутись по допомогу до батьків

В) Самій усунути несправність

* Доброго дня, я Тимур, буваючи в інтернеті, часто стикаюсь з неприємною інформацією, яка «лізе з усіх боків», вона заважає працювати в інтернеті. Як позбутися від непотрібної інформації, щоб користуватися тільки цікавими сторінками?

А) Встановити антивірусну програму

Б) Встановити фільтри на свій браузер

В) Встановити новий браузер

* Любий Незнайку, мене звати Надія. Я на уроці інформатики створила собі електронну скриньку. Тепер можу обмінюватися повідомленнями зі своїми друзями. Сьогодні на мою адресу електронної пошти прийшло повідомлення: файл з грою від невідомого користувача. Як вчинити?

А) Завантажити файл і почати грати

Б) Не відкривати файл

В) Відправити файл своїм друзям

* Хай, я Аліна і у мене проблема *–* на уроці природознавства задали знайти зображення динозаврів. Я захотіла скачати картинку в інтернеті, натиснула кнопку «завантажити», на екрані з'явилося повідомлення відправити SMS на вказаний номер в інтернеті. Відправляти чи ні?

А) Відправити СМС на вказаний номер

Б) Перевірити цей номер в інтернеті

В) Не викачувати більше картинки

* Доброго ранку. Мене звати Валентина. Вчора я познайомилася з новим другом в інтернеті, і він попросив мене терміново повідомити йому таку інформацію: номер телефону, домашню адресу, ким працюють батьки. Що я повинна зробити?

А) Повідомити йому потрібні відомості

Б) Не повідомляти в Інтернеті, а повідомити при зустрічі.

В) Порадитися з батьками

* Здрастє, Незнайчику, я вирішила опублікувати в інтернеті свою фотографію і фотографії своїх однокласників. Чи можна це зробити?

А) Ні, не можна

Б) Можна за згодою однокласників

В) Можна, згода однокласників не обов’язкова

* Привіт, мене звати Роман і мені купили комп'ютер. Тепер цілий день сиджу за ним. Через кілька днів у мене стали сльозитися очі, з'явилися болі в руках. Що робити ?

А) Продовжувати проводити час за комп’ютером

Б) Дотримуватися правил поводження за комп’ютером

В) Більше ніколи не працювати з комп’ютером.

* Незнайко, привіт, я Оленка, навчаюся в 6-б класі. Нещодавно я познайомилася в інтернеті з учнем 6-го класу Віталіком Незвичайним. Віталік не вчиться зі мною в одній школі, і взагалі я його жодного разу не бачила. Віталік запросив мене зустрітися з ним у парку. Що мені робити?

А) Піти на зустріч

Б) Піти разом з татом чи мамою

В) Не ходити на зустріч

* Здраствуй, Незнайко, я Євген. У мене дуже багато друзів в інтернеті, і я щодня додаю нових друзів у свій контакт-лист в ICQ. Раптом мені стали приходити повідомлення з неприємним, грубим змістом. Що я повинен зробити?

А) Написати образи у відповідь

Б) Не відповідати тим же, але продовжити з ним спілкування.

В) Повідомити про це дорослим.

* Привєтік, я Оксана. На уроці інформатики почула нове слово «нетікет». Але поки вчитель пояснював, я гралася в телефоні і не пам’ятаю що воно означає.

А) Правила етикету

Б) Правила роботи на комп’ютері

В) Правила мережевого етикету

**Нетікет (Netiquette)** *–* (англ. Net *–* мережа, Etiquette *–* етикет) *–* моральні правила поведінки в комп'ютерних мережах.

* Ось ми з вами повторили правила користуванням інтернетом.

1. **Вихід казкового героя.**

**Незнайко:** Всім привіт, а ось і я.

**Вчитель:** Привіт, Незнайку. Ми вже зачекались, чого ж ти запізнюєшся?

**Незнайко**: Просто скачав таку кла-а-асну гру… Грав у неї цілий день і ніч, що навіть трохи забув, який сьогодні день…

**Вчитель**: Так це ж небезпечно і шкідливо для здоров’я. Дітки, ви згодні?

**Незнайко:** Ой, та ну не розказуйте! В інтернеті так багато цікавого… і незрозумілого. Он мій друг Петрусь з нього взагалі не виходить, цілими днями зависає… ходімо до ньог,о самі переконаєтесь, можливо вмовимо його піти з нами.

**5.Перегляд мультфільму «Найжахливіший день Петрика»**

**Незнайко:** Ой, невже це правда? Н-іііі я так не хочу. Доведеться нам без Петрика почати подорож. Так?

А куди ж нам прямувати,

Що, коли і як шукати.

Допоможе нам система,

Пошукова – оце тема!

Їй задай скоріш питання,

Можеш відшукати вітання,

Це цікаво і доречно,

Лиш працюй ти в ній безпечно

**Вчитель:** Незнайку, а ти знаєш, що існують спеціальні пошукові системи для дітей, а також можна використовувати дитячий браузер Гогуль. Він гарантує безпеку дитини в інтернеті за рахунок наявності власного каталогу дитячих сайтів. Гогуль веде статистику відвіданих сайтів для контролю батьками, а також може обмежувати час перебування в інтернеті.

*Незнайко дістає гаджет*

**Незнайко:** Так, Гугль, Гагль, Грегль… щось не так?

**Діти**: Гогуль!

**Незнайко:** Гогуль, покажи як в світ інтернету потрапити!

**Незнайко:** Ну що ходімо! Два кроки направо, один наліво, три вперед і крок назад*. (Виходить за двері)*

**Вчитель:** Поки наш Незнайчик шукає шлях до інтернету, ми з вами трохи відпочинемо. Пропоную розім’яти наші м’язи обличчя і відтворити емоції за Смайликом.

**6. Гра «Відтвори емоцію Смайлика»**

Всі ви є активними користувачами соціальних мереж. І практично щодня спілкуєтеся один з одним за допомогою інтернету. Віртуальне спілкування витісняє живе. Ви навчилися виражати свої емоції в інтернеті за допомогою смайликів. А зараз ми перевіримо, чи так само вправно ви можете виразити свої емоції і в реальному житті.

(*На екрані з’являються смайли, учням потрібно відобразити ту емоцію, яку він показує)*

**Незнайко:** (*Сидить за комп’ютером і не відриває очей. Час від часу щось вигукує*) Урра!!! Таааак! Ще трііішки.

**Вчитель:** Незнайку, а як же наша подорож? Незнааайку! Здається наш Незнайко відправився у світ інтернету без нас…

(*Пауза, всі мовчат,ь вчитель час від часу говорить до Незнайка)*

Ехх, здається наш друг сильно застряг в цій всесвітній павутині… і щось мені підказує що нам буде не просто його звідти витягнути….

Ой! Що це? Хто це? Та це ж віруси та інтернет-небезпеки…

1. **Гра «Показуха»**

*Під музику один за одним заходять діти-віруси, копіюють їх поведінку. На кожному прикріплений відповідний значок.*

*****На екрані з’являються їх назви та характеристики. При потребі вчитель доповнює інформацію.*

**Учень 1. Клавіатурний шпигун** – програма, що відстежує введення користувачем паролів і пін-кодів.

**Учень 2. Хробаки** – окремий вид шкідливих програм, головною задачею яких є розмноження серед комп’ютерів в мережі.

**Учень 3. Адваре** – рекламні модулі. Ці програми, мабуть найменш небезпечні з усіх шкідливих програм, але через дуже широку розповсюдженість і просто величезну зухвалість їх авторів в останній час вони стали досить неприємними. Задача рекламного модуля – показати вам рекламу. Це може відбуватись у різних проявах, наприклад, у вас можуть самостійно відкриватись певні сторінки у браузері, які ви не відкривали – це будуть сайти з дивною рекламою або просто сайти, які ви не збирались відвідувати.

**Учень 4. Дропери** – це програми, які встановлюють троянські програми на комп’ютери користувачів.

**Учень 5. Руткіт** – це спеціальний вид троянських програм, головна мета якого – максимально глибоко інсталюватись у систему, щоб його було якомога важче знайти і видалити. Як правило, руткіти містять драйвери операційних систем. Головна проблема в тому, що руткіти дуже важко знайти і ще важче видалити з системи. Далеко не кожна антивірусна програма може з цим впоратись.

**Учень 6. Спам –** це масова розсилка реклами або іншого виду повідомлень особам, які не висловлювали бажання їх отримувати. Метою розповсюдження підроблених повідомлень є отримання від споживачів таких особистих відомостей: власного імені та імені користувача; номера телефону й адреси; пароля або PIN-коду; номера банківського рахунку.

**Учень 7. Грифери.** Інтернет-шахраї, які заважають учасникам онлайн-ігор спокійно грати. Вони періодично пошкоджують ігрових персонажів, блокують певні функції гри та викрадають як персонажів, так і їхнє віртуальне життя.

**Учень 8. Фішинг** – технологія інтернет-шахрайства, розроблена з метою крадіжки конфіденційної інформації. Різновидами її є поштовий фішинг (отримання листа від «державної установи» або «банку» із вимогою повідомити особисті дані) та онлайн-фішинг (створення ідентичної копії відомих сайтів інтернет-магазинів з метою обманювання покупців).

Наприклад, користувач хоче відкрити сайт вконтакте ру, а замість цього набирає вконракте ру. Як показує статистика такі помилки при введені адреси користувачі роблять досить багато. При цьому відкривається сторінка абсолютно схожа на сторінку авторизації популярної соціальної мережі. Користувач намагається авторизуватися, вводить свій логін і пароль, а оскільки сайт підроблений, він не авторизується, а просто повідомляє свій пароль зловмисникам.

**Учень 9. Фармінг.** Різновид шахрайства в інтернеті, коли оманливим шляхом користувач потрапляє на ідентичну копію відомих сайтів. Потім відбувається зараження комп’ютера вірусами та шпигунським програмним забезпеченням.

**Учень 10. Троянський Кінь.** **Троянські програми** — різновид шкідницького [програмного забезпечення](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F), яке не здатне поширюватися самостійно (відтворювати себе) на відміну від [вірусів](https://uk.wikipedia.org/wiki/%D0%92%D1%96%D1%80%D1%83%D1%81_%D0%BA%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B8%D0%B9) та [хробаків](https://uk.wikipedia.org/wiki/%D0%A5%D1%80%D0%BE%D0%B1%D0%B0%D0%BA_%D0%BA%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B8%D0%B9), тому розповсюджується людьми.

**Учень 11. Рекламне програмне забезпечення**

Одна із найпоширеніших шкідливих програм. Програми автоматично доносять рекламні оголошення на комп’ютери. Серед видів Adware. Деякі відносно безпечні, інші використовують інструменти для відслідковування та збору інформації про ваше місцезнаходження чи історії відвідування сайтів і виводу цільових оголошень на екран вашого комп’ютера.

**Учень 12.** **Шпигунське програмне забезпечення** – слідкує за вашими діями на комп’ютері. Воно збирає інформацію (наприклад, реєструє натискання клавіш на клавіатурі вашого комп’ютера, відслідковує, які сайти ви відвідуєте і навіть перехвачує ваші реєстраційні данні), потім відправляє третім особам, як правило, кіберзлочинцям. Може змінювати налаштування захисту на вашому комп’ютері і припиняти мережеве з’єднання.

**Учень 13**. **Програми-вимагачі –** заражають ваш комп’ютер, потім шифрують конфіденційні дані, наприклад, особисті документи чи фото, і вимагають викуп за їх розшифрування. Якщо ви відмовляєтеся платити, дані видаляються. Деякі види програм-вимагачів можуть повністю заблокувати доступ вашому комп’ютеру. Вони можуть видавати свої дані за роботу правоохоронних органів і звинуватити вас в будь-яких протизаконних вчинках.

**Учень 14.** **Боти –** це програми, призначені для автоматичного виконання певних операцій. Вони можуть використовуватися для легітимних цілей, але злочинці пристосували їх для своїх шкідливих цілей. Проникнувши в комп’ютер, боти можуть примусити його виконувати визначені команди без схвалення чи взагалі без відома користувача. Хакери можуть також пробувати заразити декілька комп’ютерів одним і тим самим ботом, щоб створити – бот-мережу, яка буде використовуватись для віддаленого керування зламаними машинами.

**Учень 15**. **Баги –** помилки в елементах програмного паролю – це не види шкідливого програмного забезпечення, а саме помилки, допущені програмістом. Вони можуть мати невиправні наслідки для вашого комп’ютера.

**Вчитель:** Що ж робити, як врятувати Незнайка? Дітки, можливо у вас є варіанти?

**Діти**: Потрібен антивірус

**Вчитель**: Так, ви маєте рацію, потрібен антивірус, але один антивірус не справиться з такою кількістю небезпек. Пропоную покликати всіх антивірусів, яких ми знаємо.

Діти: (*можливі відповіді:* *[http://softcatalog.info/sites/default/files/styles/collection_item_small_logo/public/program/logo/avast_free_antivirus_dlya_windows-logo.png](http://softcatalog.info/ru/programmy/avast-free-antivirus)Avast Free Antivirus, [http://softcatalog.info/sites/default/files/styles/collection_item_small_logo/public/program/logo/avg_anti-virus_free_dlya_windows-logo.png](http://softcatalog.info/ru/programmy/avg-anti-virus-free) AVG Anti-Virus Free,*

*[http://softcatalog.info/sites/default/files/styles/collection_item_small_logo/public/program/logo/panda_antivirus_pro.png](http://softcatalog.info/ru/programmy/panda-antivirus-pro) Panda Antivirus Pro, [http://softcatalog.info/sites/default/files/styles/collection_item_small_logo/public/program/logo/iobit_malware_fighter-logo.png](http://softcatalog.info/ru/programmy/iobit-malware-fighter) IObit Malware Fighter, [http://softcatalog.info/sites/default/files/styles/collection_item_small_logo/public/program/logo/360_total_security.png](http://softcatalog.info/ru/programmy/360-total-security)360 Total Security,*

*[http://softcatalog.info/sites/default/files/styles/collection_item_small_logo/public/program/logo/eset_nod32_smart_security_.png](http://softcatalog.info/ru/programmy/eset-nod32-smart-security) ESET NOD32 Smart Security, [http://softcatalog.info/sites/default/files/styles/collection_item_small_logo/public/program/logo/antivirus_kaspersky_free_dlya_windows-logo.png](http://softcatalog.info/ru/programmy/antivirus-kaspersky-free) Antivirus Kaspersky Free ,*

*[http://softcatalog.info/sites/default/files/styles/collection_item_small_logo/public/program/logo/avira_free_antivirus.png](http://softcatalog.info/ru/programmy/avira-free-antivirus) Avira Free Antivirus, [http://softcatalog.info/sites/default/files/styles/collection_item_small_logo/public/program/logo/bitdefender_antivirus_free_edition_.png](http://softcatalog.info/ru/programmy/bitdefender-antivirus-free-edition) Bitdefender Antivirus Free Edition,*

*[http://softcatalog.info/sites/default/files/styles/collection_item_small_logo/public/program/logo/comodo_antivirus_0.png](http://softcatalog.info/ru/programmy/comodo-antivirus) Comodo Antivirus,[http://softcatalog.info/sites/default/files/styles/collection_item_small_logo/public/program/logo/dr.web_antivirus_dlya_windows-logo.png](http://softcatalog.info/ru/programmy/drweb-antivirus)Dr.Web Antivirus,*

*****Zillya! PC Tools ThreatFire****,* ***PC Tools AntiVirus Free,***

**

***Emsisoft Anti-Malware, Security Essentials***

*Діти-антивіруси виходять, щойно почують свою назву.*

**8.Тести від антивірусів**

**Аваст:** Доброго дня, дорогі друзі, що у вас сталося, нащо викликали нас?

**Касперський:** Та можете вже не відповідати, самі все бачимо*(показує рукою на Незнайка та віруси, які тягнуть Незнайка в різні боки).*

**Зілля:** Тааак (*почісує потилицю*), тууут справ на цілий тиждень. Чи, можливо, і на місяць.

**Есет:** Діти, можливо ви нам допоможете?

От і чудово, тоді ми будемо читати питання і декілька відповідей на них, а ви, щойно почуєте правильну відповідь, починайте плескати в долоні і тупати ногами, тоді віруси злякаються і втечуть, а з тими, що залишаться, ми розберемося вже самотужки. Домовились?

1. Як визначити, що ваш комп'ютер заражений?

1. Друзі отримують від вас по електронній пошті повідомлення, яких ви не посилали.
2. Комп'ютер часто зависає або програми починають виконуватися повільніше .
3. На диску зникають або змінюють назву файли і теки.
4. Комп'ютер видає несподівані звуки.
5. Усе вище перелічене

**(***Втікає АДВАРЕ)*

2. Що треба зробити в першу чергу, якщо комп'ютер піддався атаці?

1. Зробити декілька глибоких вдихів і прийняти вітаміни.
2. Дівчатам випити склянку води, а матусям – з'їсти не менше двох шоколадок.
3. Викликати міліцію і швидку допомогу, в особливо складних випадках ще і пожежних.
4. Відключити комп'ютер від інтернету.
5. Вимкнути до приїзду фахівців монітор.

*(Втікає БОТ)*

3. Яку мету переслідує така загроза, як фішинг?

1. Перенаправляти будь-які запити користувача у браузері на хакерський сайт про риболовлю.
2. Довести користувача до самогубства шляхом постійного виведення повідомлення «купи слона».
3. Обманним шляхом вивідати у користувача дані, що дозволяють отримати доступ до його облікових записів.
4. Використання вод світового океану для глобального поширення шкідливих вірусів.

*(Втікає ФІШИНГ)*

4. Троянська програма небезпечна тим, що:

1. Проникає на комп'ютер під виглядом корисної програми і виконує шкідливі дії без відома користувача .
2. Змушує користувача повертати борги.
3. Шукає на диску якогось коня, знижуючи продуктивність системи.
4. Постійно читає вголос невиразно «Іліаду» Гомера.
5. Має усі вище перелічені можливості.

*(Втікає ТРОЯНСЬКИЙ КІНЬ)*

5. Чим відрізняється комп'ютерний вірус від комп'ютерного черв'яка?

1. Нічим.
2. Черв'як не виконує шкідливих дій.
3. Черв'яки можуть ділитися, віруси – ні.
4. Вірус не є самостійним файлом.
5. Вірус здатний заразити людину, черв'як – ні.

*(Втікає ХРОБАК)*

6. Чому безпровідна мережа потребує захисту?

1. Повітря містить багато шкідливих мікробів, вірусів і інфекцій.
2. Знижується швидкість роботи з одночасним зростанням рахунків провайдера інтернету.
3. Хакери отримують за злом звичайної мережі 1 бал, за злом безпровідної – 3.
4. Це поширена помилка, безпровідна мережа не потребує захисту.
5. Незахищена безпровідна мережа витрачає значно більше електрики.

*(Втікають РЕКЛАМНЕ і ШПИГУНСЬКЕ ПРОГРАМНІ ЗАБЕЗПЕЧЕННЯ)*

**Аваст**: Ну, а з цими зараз ми швиденько справимось!

**Панда**: За роботу, друзі!

*(Антивіруси відтягують вірусів від Незнайка і виводять з приміщення)*

**Незнайко:** (*Немов прокинувшись від сну*)

**Не можу уявити життя без інтернету,

Що всі куточки світу заплів в свої тенета.

Лиш кнопку я натисну – відкриються в вікні

Новин велика збірка, і правила, й статті.

Встають переді мною найвищі в світі гори.

Ліси стоять стіною, хлюпочуть хвилі моря.

Я побуваю в шахті і в космос піднімуся.

З подругою в контакті я легко поділюся.

Та є у «павутині» картинки нехороші,

І сайти підозрілі, настроєні вороже.

А є й такі там сайти, мов вовк в овечій шкурі –

Поки їх розпізнаєш, вони тебе обдурять.

Учись добру в мережі, шукай знання й новини,

А сайти злі, що брешуть, обходить ми повинні.

**9.Підсумок заходу.**

**Вправа «*Віднови правило*»*.***

*(Учням роздаються правила, розрізані навпіл. Спочатку піднімається і зачитує учень, у якого цифра 1 і початок правила, потім учень у якого продовження цього правила і т. д.)*

1. Поводьтеся чемно і ніколи не ображайте інших!
2. Не зустрічайся із незнайомими онлайн-друзями особисто!
3. Користуйтеся пошуковими системами для дітей.
4. Уважно поводьтеся з паролями: використовуйте складні паролі, не користуйтесь одним паролем для всіх акаунтів, періодично змінюйте паролі.
5. Уважно ставтеся до посилань в повідомленнях у соціальних мережах та у інших месенджерах.
6. Встановіть антивірус одразу після встановлення операційної системи і постійно його оновлюйте.
7. При проведенні будь-якої фінансової операції через інтернет уважно дивись на протокол з’єднання. Потрібно, щоб сайт мав 'https://' протокол. Сайти, які можуть викрадати дані, працюють використовуючи протокол з’єднання 'http://'.
8. По можливості не робіть он-лайн покупки в незнайомих і маловідомих магазинах. При покупці дивіться на відгуки та рейтинг продавців.
9. Періодично робіть резервне копіювання важливої інформації.
10. Нікому і ніколи не повідомляйте персональні дані.
11. Періодично перевіряйте ваші мобільні пристрої на предмет додаткових програм, можливо ви помітите незнайомі іконки на головному екрані чи в меню смартфона.

**10. Заключне слово вчителя.**

Інтернет став невід’ємною частиною нашого життя. Цілком ймовірно, що у найближчому майбутньому Всесвітня мережа повністю замінить усі інші засоби зв’язку. Вчіться користуватись інтернетом із розумом.

Бажаю усім, щоб комп'ютер став вашим другом і помічником, і ви отримували від користування ним лише користь і ніякої шкоди.

**Використані джерела**

1. Діти в Інтернеті: як навчити безпеці у віртуальному світі: посібник для батьків / І. Литовченко, С. Максименко, С. Болтівець [та ін.]. – К.: ТОВ «Видавничий будинок «Аванпост-Прим»», 2010. – 48 с.
2. Виховання культури користувача Інтернету. Безпека у всесвітній мережі: навчально-методичний посібник / А. Кочарян, Н. Гущина. – К., 2011. – 100 с.
3. Українська молодь не може жити без Інтернету [Електронний ресурс] / Офіційний сайт інформаційного агентства УНІАН. – Режим доступу: <http://www.unian.ua/society/779261-ukrajinska-molod-ne-moje-jiti-bez-internetu-doslidjennya.html.>

