Тема тренінгу. **Безпека дітей в Інтернет** (9-11 клас)

Мета. Розширити й поглибити знання про безпечний Інтернет; розвивати уважність, спостережливість, мовленнєві навики, пам'ять, виховувати любов до родини, навколишнього світу, етичне спілкування між товаришами, дорослими, молодшими друзями.

Обладнання: комп'ютер, папір, олівці, ручки, стікери

Хід тренінгу

1. Викладач. _Вітаю всіх студентів, гостей. Сьогодні поговоримо про Інтернет, про безпеку дітей в Інтернет. В лютому цього року вже вп'яте відзначають День безпечного Інтернету завдяки ініціативі компанії «Microsoft Україна» . Ця організація є засновником веб-ресурсу «Он-ляндія – безпека дітей в Україні».

   Спочатку домовимось про декілька правил для успішної роботи:

   1. моб. телефони відключити
   2. говорити все, що думаєте
   3. слухати інших, поважати себе та інших
   4. бути активним учасником (якщо вправи виявляться для вас з якихось причин не прийнятними, попрацюйте над створенням сенкану на тему інтернету – наприкінці тренінгу ми послухаємо ваші твори.)

2. Викладач. Оголошую мозковий штурм «Про користь Інтернету». Відтворити ваші думки на дошці мені допоможе студентка.

   Отож, користь очевидна.

3. Викладач. Поговоримо про рівень обізнаності українців щодо безпеки дітей в Інтернеті

У 2011 році у рамках програми Microsoft «Партнерство в навчанні» кафедрою превентивної роботи та соціальної політики ЮНЕСКО в Україні було проведено Всеукраїнське широкомасштабне дослідження «Рівень обізнаності українців щодо питань безпеки дітей в Інтернеті». Детальне дослідження вперше було проведено в Україні.

Ключові результати:

З 96% дітей-користувачів Інтернету віком від 10 до 17 років 51% не знає про небезпеки в мережі.

52% дітей виходять в Інтернет передусім для спілкування у соціальних мережах, де залишають свій номер мобільного телефону (46%), домашню адресу (36%), особисті фото (51%).

44% дітей знаходяться у потенційній зоні ризику (розміщують особисту інформацію) і 24,3% вже були в ризикованих ситуаціях (ходили на зустріч з віртуальними знайомими). У віковій групі від 15 до 17 років цей показник досягає 60,3%.

72,5% дітей хочуть отримувати більше інформації про те, як убезпечити себе в Інтернеті. 77% батьків також висловили бажання більше дізнатися про безпеку Інтернету для дітей.

У сім'ях діти краще за батьків розбираються у комп'ютері та Інтернеті. З 81% батьків, у яких на домашньому комп'ютері є антивірус, 95% зазначили, що його установкою і налаштуванням займалася дитина.

Дослідження показало: що дорослішою стає дитина, то більш безтурботно вона починає поводити себе в Інтернеті. Так, на реальну зустріч з людиною, з якою знайомі лише віртуально, вже ходили майже 12% опитаних дітей віком 10-11 років та більше ніж 60% підлітків 15-17 років (графік 1). Дані про своїх батьків у мережі (місце роботи, посада) залишили 0,4 дітей віком 10-11 років та 6,5% 15-17-річних (графік 2).

Найпопулярніші за відвідуваністю серед дітей ресурси в Інтернеті – соціальні мережі – містять найбільшу загрозу з точки зору доступності особистої інформації для сторонніх осіб. У соціальних мережах свій особистий номер телефону вже залишили 46% дітей 10-17 років, вказали домашню адресу – 36%, розмістили особисті фотографії – 51%.На які ризики діти наражають себе в Інтернеті?

Наші експерти підготували чималий список. Прислухайтесь і зробіть доповнення

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 саморозмноження 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.

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 ранні ми ознаками зараження комп'ю тера вірусом є:

- зменшення обсягу вільної оперативної пам'яті;
- уповільнення роботи комп'ютера та завантаження;

- незрозумілі (без причин) 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» кон тент, яки й можуть переглядати діти, зокрема порноконтент. Розміри порноіндустрії неможливо навіть виміряти. Вона вважається третім великим джерелом прибутку для організованої злочинності в США, яка отримує від 8 до 10 більйонів доларів у рік (за даними 1986 року). Інтернет може надати дітям швидкий та (у більшості випадків) безкоштовний доступ до порноконтенту. Необхідно лише ввести ключові слова або фрази для того, аби отримати тисячі посилань на сайти із дорослим контентом. Практично гарантовано, що дитина зіткнеться із порноконтентом, навіть якщо вона і не шукала його.

Пропагування сексуального насилля над дітьми, жорсткої поведінки, шкідливих звичок тощо.

Перегляд матеріалів, що містять сцени насилля та жорсткості по відношенню до людей або тварин, перешкоджає нормальному формування моральних цінностей та може завдати психологічних травм.

Он-лайн-звабления 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 та жертвою відбувається під час спілкування в мережі Інтернет: миттєві повідомлення, блоги, соціальні мережі, дошки оголошень та інше.

Кібер-хуліганство. Кібер-хуліганство – 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 кібер-хуліганства можна й у власній оселі на очах у батьків. Варіанти кібер-хуліганства досить різноманітні. Основними їх різновидами є наступні.

Кібер-булінг. Одна із форм переслідування дітей та підлітків за допомогою ІКТ. Для цього можуть створюватися сайти, на яких розм іщуються матері али, що комп рометують д итину (ф ото, відеозйомки тощо). З метою кібер-булінгу використовуються сервіси миттєвих повідомлень, електронна пошта, соціальні мережі, ігрові та розважальні сайти, соціальні мережі, форуми та чати

Кібер-грумінг. Цей термін розкриває суть ще одного різновиду кібер-хуліганства – 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 кібер-грумінгу - наполегливе чіпляння в мережі із сексуальними пропозиціями, розмови на теми сексу, насильства та (або) виготовлення, розповсюдження і використання матеріалів зі сценами насильства над дітьми (у більшості випадків – сексуального).

Грифери. Інтернет-шахраї, які заважають учасникам он-лайн-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.

Це відбувається завдяки використанню пев них Інтернет-технологій.

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;
- Web-сторінки, 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 та здійснення атак на інші комп'ютери та сервери.

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 он-лайн-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.

Он-лайн-хижаки

«Хижаки» встановлюють контакт із дітьми шляхом розмов у чат-кімнатах, обміну миттєвими повідомленнями, електронною поштою або через дошки повідомлень. Багато підлітків користуються он-лайн-форумами підтримки ровесників з метою вирішення власних проблем. Хижаки часто відвідують такі зони в он-лайні, щоб знайти вразливих жертв. Он-лайн-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. Деякі «хижаки» працюють щвидше, одразу ж втягуючи дітей у розмови на сексуальну тему. Цей більш прямолінійний підхід може включати і сексуальне домагання. Хижаки також можуть спонукати дітей, з якими вони знайомляться в он-лайні, до контакту віч-на-віч. Найбільш вразливими для он-лайн-хижаків є молоді люди, яким притаманні такі риси:

- вони новачки в он-лайні й незнайомі з «мережевим етикетом»;
- завзяті користувачі комп'ютера;
- хочуть спробувати у житті щось нове, авантюрне;
- активно шукають уваги та дружби;
- бунтівні;

- їх приваблюють субкультури, що існують за межами їхнього власного контрольованого батьками світу.

Створення у мережі профайлів для виявлення інтересів дитини

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

Це масова 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 валідац її кредитної ка ртки (CVC) а бо іден ти ф іка цій ного зн аченн я ка ртки (CVV); коду соціа льн ого 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. Спам також може розсилатися завдяки використанню наступних Інтернет-ресурсів.

Недостовірна інформація

Вчителі загальноосвітніх навчальних закладів 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 студенти завантажують вже готові реферативні повідомлення з Інтернету та роздруковують їх. Це займає часу максимум 1 годину. Проте часто студенти 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 (і ми знаходили) інформацію, яка є не лише антинауковою, а й життєво небезпечною, якщо нею скористатися.

Викладач . Дослідження показало: що дорослішою стає дитина, то більш безтурботно вона починає поводити себе в Інтернеті. Так, на реальну зустріч з людиною, з якою знайомі лише віртуально, вже ходили майже 12% опитаних дітей віком 10-11 років та більше ніж 60% підлітків 15-17 років(графік 1). Дані про своїх батьків у мережі (місце роботи, посада) залишили 0,4% дітей віком 10-11 років та 6,5% 15-17-річних (графік 2).

4 Викладач. Обговоримо , як правильно та безпечно використовувати Інтернет

5 Вправа «Квітка»

Вигадати собі нікнейм або вказати існуючий, записати на стікер, приклеїти як пелюстку до квітки. Назвати свої ім'я та прізвище і нікнейм.

6 Вправа «Хто надіслав листа?»

Написати позитивне побажання і приклеїти стікер до квітки, поруч із пелюстками. Власники нікнеймів відгадують, хто їм надіслав листа. *В інтернет просторі важко зрозуміти, хто знаходиться по той бік комп'ютера*

7 Вправа «Баскетболіст забив два м'ячі одним ударом»

Декілька учасників виходять за двері. Першому учаснику тренер говорить фразу: «Баскетболіст забив два м'ячі одним ударом». Заходить один учасник. Перший за допомогою жестів передає йому цю фразу, яку той повинен записати на папері так, як він її зрозумів. Потім він показує жестами те, що сам зрозумів і записав на папері, ітак далі. У фіналі зачитуються всі фрази, починаючи від останньої ізакінчуючи найпершою.
Тренер пропонує відповісти на декілька запитань:

- Чи вдалося вам зберегти перший варіант ? Чому? Що Вам допомагало? Що вам заважало?

8 Вправа «Друкарська машинка»

Учасники шикуються в одну лінію. Тренер озвучує рядок із вірша, який необхідно «надрукувати».

В неволі, в самоті немає,
Нема з ким серце поєднати.
То сам собі оце шукаю
Когось, аби порозмовляти.
Учасники називають по одній літері: 1-й – В, пропуск – всі плескають у долоні, 2-й – Н, 3-й – Е, 4-й – В і так далі.
Якщо учасник помиляється, то він вибуває з гри, а всі решта починають спочатку.

Мережа Інтернет – швидкий віртуальний світ, в якому постійно треба мати концентровану увагу, щоб не потрапити у халепу.

9 Вправа «Кубик»

Тренер до початку тренінгу готує 7 аркушів паперу форматом А-4, на яких пише великі цифри від 1 до 7. Ці аркуші тренер розклеює в різних кутках кімнати, але так, щоб усі учасники мали змогу їх побачити. Не можна розміщувати цифри у порядку їх лічби: 1 не може бути поруч із 2.

Тренер декілька разів наголошує на тому, що зараз учасники візьмуть участь у грі.

Тренер повідомляє, що для кожного із учасників він мав підготувати сувенірну продукцію, але виявилося, що їх на тренінг з'явилося більше, аніж тренер планував, і тому деякі учасники мусять залишитися без подарунків. Але все повинно бути по-чесному, і тому зараз треба буде вирішити, хто ж саме додому піде без подарунка. Учасникам пропонується обрати будь-яку цифру, яка, на їхню думку, буде щасливою для них. Під час гри суворо забороняється розмовляти та підказувати один одному: кожен грає мовчки. Після того, як учасники обрали свої цифри, тренер ще раз наголошує на тому, що під час гри не можна розмовляти, і дістає кубик.

Тренер говорить, що за допомогою кубика він і обере ту групу, яка не отримає сьогодні подарунка. Тренер підкидає кубик і підходить до групи, яка обрала ту цифру, що випала на кубику. Тренер звертається лише до членів цієї групи: «Які ваші враження?», «Як ви гадаєте, що зараз думають інші учасники тренінгу?». Потім тренер каже, що це була репетиція, і тому учасники цієї команди мають можливість змінити цифру. Після цього тренер

пропонує змінити цифру всім учасникам, які мають таке бажання. Коли вибір зроблено, тренер знову підкидає кубик і звертається до команди, цифра якої випала на кубику: «Які ваші враження?», «Як ви гадаєте, що зараз думають

інші учасники тренінгу?». Тренер повідомляє гарну новину: це була ще одна спроба, і учасники ще раз можуть змінити цифру. Гра триває до тих пір, доки тренер не помітить, що учасники під цифрою «7» не змінюють свого місця. І не даремно – на кубику немає цифри 7! У цей момент тренер перериває гру і звертається до учасників, що обрали цифри «2», «3», «5»: «Що ви відчували кожного разу, коли я підкидав кубик?» Учасники зазвичай будуть казати, що хвилювалися. Потім тренер звертається до учасників під цифрою «7» з тим самим

запитанням. Але учасники, які обрали цю цифру, скажуть, що не турбувалися про те, яка цифра випаде на кубику, бо цифри 7 там немає! Сенс гри полягає в тому, щоб учасники якомога швидше усвідомили правила цієї гри і перейшли до цифри 7.

Учасники міцно усвідомлять, що знання правил і дотримання їх – це різні речі, і тільки дотримання правил приносить винагороду.

10 Вправа «Корова».

6 учасників зі стільцями. Ділити на талановитих і красномовних. Учасник, який має малюнок, не повинен показувати його своєму партнерові, а виключно словами передати зміст зображеного. Учасник, який має чистий аркуш паперу та олівець, повинен якомога точніше намалювати те, що буде казати його напарник, тобто зробити свою копію малюнка.

11 Вправа «Термінатор»

Кількість учасників гри повинна бути кратна трьом. Тренер пояснює правила. Всі учасники беруть участь у грі. Вони отримують стікери різного кольору і наклеюють їх на свій одяг. Завдання полягає в тому, щоб не загубити і не втратити ці стікери. Тренер буде показувати на будь-кого з учасників та давати команди: «міксер!», «пральна машинка!», «слон!», «тостер!». На кожну команду всі учасники повинні виконати відповідні дії. Наприклад, тренер показує на одного учасника та промовляє: «Міксер!» Учасник, на якого показав

тренер, піднімає руки та ромовляє голосно звук «вжик», а учасники зліва та справа рухаються навколо своєї осі під його руками. Усі інші пропорційно розміщуються по троє і також виконують ці дії. Якщо лунає команда «пральна машинка!», учасник, на якого показав тренер, починає крутити головою, а ті, що знаходяться зліва та справа, руками роблять велике коло, в якому і крутить головою їхній партнер по грі. Всі інші учасники пропорційно розміщуються по троє і також виконують ці дії. Команда «слон!», і учасник, на якого показав тренер, витягує вперед складені руки («хобот»), а учасники зліва та справа імітують руками великі вуха слона. Решта пропорційно розміщуються по троє і також виконують ці дії. Звучить команда «тостер!», і учасник, на якого показав тренер, починає підстрибувати на одному місці, а учасники зліва та справа складають руки та піднімають їх вгору. Між цими руками і плигає «тост». Всі інші учасники пропорційно розміщуються по троє і також виконують ці дії. Тренер повідомляє тільки 2-3 обраним учасникам їхнє особливе завдання. Як тільки тренер скаже «термінатор!», ці учасники повинні якомога швидше забрати стікери в інших учасників. Коли учасники добре зрозуміли правила гри і швидко орієнтуються після кожної команди, тренер несподівано для всіх дає команду «термінатор!». Звісно, більшість учасників не розуміє, яку саме дію треба виконувати. Але в цей час 2-3 учасники, які знають нюанси гри, користуючись розгубленістю решти учасників, швидко забирають стікери, які всі, згідно з правилами, повинні пильно берегти. У результаті більшість із них втратить свої стікери – їх заберуть «термінатори», яким із самого початку були відомі всі правила гри. Обговорення.

- Чи сподобалася вам гра? Чому? (учасники не знали всіх правил).

- Чому ви не зберегли свої стікери? Що вам заважало?

- Чи незнання правил гри може виправдати той факт, що ви не зберегли стікери, адже ви чітко знали умову гри: берегти стікери?

Аналогія з мережею Інтернет. У більшості випадків діти, відвідуючи сайти із дорослим або небажаним для них контентом, не усвідомлюють тих небезпек,

на які можуть наразитися. Мета авторів цих сайтів – ввести дітей у такий психологічний стан, щоб вони втратили пильність. Оскільки діти не знають справжньої мотивації авторів цих сайтів, вони досить легко можуть потрапити у халепу.

12 Підсумок. Сенкани від експертів та бажаючих.