МЕТОДИЧНА РОЗРОБКА НАВЧАЛЬНО-ВИХОВНОГО ЗАХОДУ

у 9-11 класі Тилявського НВК
проведеного 13 лютого 2014 року
на тему: «ІНФОРМАЦІЙНА БЕЗПЕКА»

підготував і провів
студент-практикант V курсу
фізико-математичного факультету
Смоляк Віктор Васильович

Навчально-виховний захід

«ІНФОРМАЦІЙНА БЕЗПЕКА»

Дата проведення: 13 лютого 2014 року;

Середній вік учасників (клас): 9-11 класи;

Кількість учасників: 15;

Аргументація/актуальність: ознайомити учнів з можливими загрозами, що чекають учнів в мережі та дати поради щодо захисту і етикету в Інтернеті;

Мета (освітня, виховна і розвиваюча): Розглянути можливості використання Інтернету; познайомити учнів з можливими загрозами, що чекають учнів в мережі та дати поради щодо захисту і етикету в Інтернеті. Розвивати логічне мислення учнів. Виховувати інформаційну культуру учнів.

Форма виховного заходу: навчально-виховний, тренінг

Використане обладнання: презентація «Інформаційна безпека в мережі Інтернет».

Список використаної літератури:

1. **http://teacherjournal.com.ua/shkola/informatika/17713-nformaczjna-bezpeka-v-merezh-nternet.html – Інформаційна безпека в мережі Інтернет**
2. **http://szosh3.ucoz.ru/_ld/0/32_Trening.doc – Виховний захід. Інформаційний тренінг на тему: «Твоя інформаційна безпека»**
3. **http://uk.wikipedia.org/ – Вікіпедія.**

Гра-фантазія „Уяви!"

Заплющте, будь ласка, на хвильку очі! Навколо темрява, холодно, страшно. Морок ночі огортає вас... У таких умовах протягом шести місяців

дослідник Антарктиди Роберт Бард жив сам. У своєму щоденнику він писав: „У мене є запас води та їжі, є спокій, якого я так прагнув. Але не можу обійтися без звуків, голосів та найголовнішого - спілкування!"

Уявіть, як змінилося б життя дослідника, якби він міг користуватися телефоном, міг отримувати газети або журнали, мав телевізора або радіо. (Відповіді учнів)

- Отже, ви зрозуміли, що людині дуже важливо спілкуватися з іншими людьми: отримувати інформацію та ділитися нею. Та ви знаєте про випадки коли переглянувши якийсь фільм, телепередачу, прочитавши оповідання із страшним сюжетом, людина погано себе почуває. Чому? Чи може інформація бути шкідливою, неякісною? Сьогодні ми постараємось відповісти на ці питання.

Формування понять.

Інформація-це відомості про об'єкти навколишнього світу, які сприймаються людиною або спеціальними пристроями і підвищують їх рівень інформативності. Швейцарський мислитель кінця XVIII століття Лафа тер зауважував: „Хочеш бути розумним-навчися розумно запитувати, уважно слухати, спокійно відповідати, переставати говорити, коли нема чого більше сказати".

Сьогодні вже нікого не здивуєш комп'ютером. Але були часи, коли про комп'ютери можна було прочитати лише в фантастичній літературі. Перший комп'ютер був зроблений під час другої світової війни. Завдяки йому розшифровувались секретні коди. Він займав майже цілу кімнату, адже його комплектуючі були дуже великими. Згодом, протягом 50-х — 60-х років XX - сторіччя вчені винаходили все більш компактні блоки, і, завдяки цьому, тисячі таких блоків змогли вміститися в простір розміром з ніготь людини. Інтернет.

Інтернет - видатний винахід сучасності. Це світова мережа, яка дозволяє єднати мільйони комп'ютерів в різних куточках світу. Наприкінці 50-х років XX століття, під час «Холодної війни» в СІЛА в військових дослідах використовувались комп'ютери. Саме там прийшла ідея з'єднати декілька обчислювальних машин в мережу. Але здійснити ідею вдалося через 10 років - в грудні 1969 року, коли в мережу, що назвали назву ARPAnet, з'єднали комп'ютери 4 американських університетів. Згодом мережі з'явилися і в інших країнах - в Англії, Норвегії, Японії. Наступним кроком був винахід спеціального комп'ютерного протоколу, інакше кажучи, мови, завдяки якій змогли спілкувалися комп'ютери різного типу і мереж. Так і з'явився Інтернет. (Зерновою Інтернету є потужні комп'ютери-сервери, які постійно ввімкнені та з'єднані один з одним. Саме вони обробляють та направляють потік інформації всесвітньої мережі.

Мозковий штурм «Що я повинен знати про Інтернет»

(для актуалізації знання і досвіду учнів)

1. **Що таке комп'ютерна мережа?**
2. **Що таке Інтернет?**
3. **Які сервіси Інтернету Вам відомі?**

Користуючись Інтернетом чи часто Ви задумувались:

1. **Чи безпечний Інтернет?**
2. **Які загрози приховуються в ньому?**
3. **Яким чином захиститися в мережі Інтернет?**

Вивчаючи дану тему ми з'ясуємо які небезпеки приховані в Інтернеті, як захистити себе в мережі…

Інтернет – не тільки 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. Соціальні мережі, чати, форуми сайти-знайомств та інші сайти приховують багато небезпек . Знання цих небезпек дозволить їх уникнути.

Розповідь з обговоренням.

Комп'ютерний вірус – це невелика програма, яка має здатність розмножуватися та знищувати інформацію, блокувати роботу комп'ютера. На сьогоднішній день відомо понад 50 тисяч вірусів і їх кількість зростає кожного дня. Проявляється дія вірусів на комп'ютері по різному: уповільнення роботи, затримки при виконанні програм, незрозумілі зміни у файлах, зникнення файлів, візуальні ефекти, форматування жорсткого диска, незрозумілі системні повідомлення та звукові ефекти, самовільне відкривання браузером деяких сайтів (рекламного характеру) та інше. Одним із видів вірусів є **хробаки.** Вони схожі на віруси, так як розмножуються і роблять власні копії, але на відміну від вірусів не потребують носія і передаються здебільшого через електронну пошту. Хоча спершу хробаки були не були шкідливими, нинішні їхні різновиди спричиняють значні перезавантаження мереж і можуть руйнувати файли. Так, вірус Mellisa, перший з тих, що атакували системи електронної пошти, з моменту своєї появи в 1991 році заподіяв збитків на 80 млн. длр.

Хакери та крекери.

Хакер (від англ. to hack — рубати) — особливий тип комп'ютерних спеціалістів. Нині так часто помилково називають комп'ютерних хуліганів, тобто тих, хто здійснює неправомірний доступ до комп'ютерів та інформації. Інколи цей термін використовують для позначення спеціалістів взагалі — у тому контексті, що вони мають дуже детальні знання в якихось питаннях, або мають достатньо нестандартне і конструктивне мислення. З моменту появи цього слова в формі комп'ютерного терміну (започаткованого в 1960-ті роки), в нього з'явилися достатньо різноманітні значення. Обдарований програміст, ентузіаст своєї справи, прихильник свободи та відкритості інформації.

Крекер — спеціаліст в області комп'ютерних технологій, діяльність якого пов'язана з намаганням отримати несанкціонований доступ до систем із секретною (конфіденційною) інформацією, комп'ютерний злочинець.

Одним із інструментів хакера та крекера є троянський кін.

Троянський кінь – це комп'ютерні програми, які добре вміють маскуватися під програмні продукти, а насправді виконують різні користувачем дії (збирають та пересилають, змінюють або псують інформацію, використовують ресурси комп'ютера на власний розсуд).[3]

Ці віруси самостійно не розмножуються. Вони видають себе за корисні програми, провокуючи користувача самостійно їх встановити.

Окремі категорії троянських вірусів здатні завдавати збитків віддаленим комп'ютерам та мережам, не порушуючи працездатності зараженого комп'ютер

Ботнет (англ. botnet від robot і network) — це комп'ютерна мережа, що складається з деякої кількості хостів, із запущеними ботами — автономним програмним забезпеченням. Найчастіше бот у складі ботнета є програмою, яка приховано встановлюється на комп'ютері жертви і дозволяє зловмисникові виконувати певні дії з використанням ресурсів інфікованого комп'ютера. Зазвичай використовуються протиправної діяльності — розсилки спаму, перебору паролів на віддаленій системі, атак на відмову в обслуговуванні, отримання персональної інформації про користувачів, крадіжка номерів кредитних карт та паролів доступу.

Комп'ютер може потрапити в мережу ботнету через встановлення певного програмного забезпечення, без відома користувача. Трапляється це зазвичай через:

Інфікування комп'ютера вірусом через вразливість в ПЗ (помилки в браузерах, поштових клієнтах, програмах перегляду документів, зображень, відео).

Недосвідченість або неуважність користувача — шкідливе ПЗ маскується під "корисне програмне забезпечення".

Використання санкціонованого доступу до комп'ютера (рідко).

Спам.

Спам (англ. spam) — масова розсилка кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати. Передусім термін «спам» стосується рекламних електронних листів. Також вважаються спамом освідчення в коханні на електронну пошту, в чатах, соціальних мережах і т.п. Найчастіше спам використовують для розсилання реклами, але є й інші сфери його застосування:

- реклама незаконної продукції
- нігерійські листи (ноді 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.)
- фітинг
- масове розсилання листів релігійного змісту
- масове розсилання листів, містять комп’ютерні віруси
- масове розсилання листів з метою виведення комп’ютерної системи із ладу.

Інтернет шахрайство.

Сказати що в Інтернеті існує шахрайство – це не сказати нічого. Інтернет – це рай для шахрайства.

1. Фальшиві товари на аукціонах

На онлайн-аукціонах типу eBay досить часто попадаються фальшиві товари. І незважаючи на те, що в того ж eBay є комісія для відстеження

шахраїв, однаково ймовірність купити підробку існує, навіть якщо надані сертифікати, котрі підтверджують справжність.

Ще на інтернет-аукціонах бувають випадки накручування ціни за допомогою спільників. Продавець з іншого акаунту або його друзі підвищують ставку, щоб ви заплатили більше. Тому якщо якийсь користувач часто трапляється у списку тих, що зробили ставки в одного продавця, можливо, він просто накручує ціну. І ще одне: ніколи не переказуєте гроші за товар напряму. Якщо вам нічого не надішлють, повернути гроші в такому випадку буде практично неможливо.

2. Банківська афера, або фішинг

Якщо ви отримали електронного листа від свого банку, в якому сказано, що хтось намагався скористатись вашим рахунком, і для розблокування рахунку вам необхідно передати банку інформацію, що підтверджує особу, у жодному разі не слід цього робити. Банки ніколи не запитують таку інформацію через е-мейли. Аферисти (фішери), отримавши вашу особисту інформацію, скористаються нею для одержання доступу до вашого ж банківського рахунку.

3. Афера «Ви виграли безкоштовний подарунок!»

Щоразу, коли вам в Інтернеті безкоштовно пропонують те, за що зазвичай треба платити, варто бути вкрай обережним. Виробники товарів, які ви «виграли, отримавши е-мейл» – комерційні організації, і в їхні плани не входить роздавати тисячі гаджетів безкоштовно. У таких аферах звичайно просять оплатити тільки доставку, якої, природно, не буде.

4. Благодійна афера

Як тільки трапляється трагедія, що вимагає доброчинності, активізуються не тільки благодійні фонди, але й аферисти. Якщо вам приходить е-мейл із проханням про внесок, не варто зразу пересилати гроші. Впевніться на 100%, що ці кошти підуть куди треба. А взагалі в таких випадках краще довіряти великим благодійним організаціям, таким як Червоний Хрест або Міжнародна амністія.

5. Шантаж

Іноді трапляється, що «жертві» приходить лист із погрозами викрадення кого-небудь із близьких і вимогами перерахувати енну сумі грошей на рахунок відправника листа. Звичайно ж, це афера. Навіть якщо ви відчуваєте, що хтось справді може викрасти ваших родичів або має у розпорядженні компромат, найкраще звернутися в правоохоронні органи.

Буває й зворотна ситуація: вам приходить лист від сищиків, які знайшли ваші контакти в затриманого злочинця, і просять допомогти в розслідуванні. Насправді аферисти просто виманюють у вас особисту інформацію.

Online-хижаки

Використання таких інструментів комунікації в Інтернеті, як чат-кімнати, електронна пошта та обмін миттєвими повідомленнями, може поставити дитину під потенційну загрозу зустрічі з он-лайн-хижаками. Анонімність Інтернету означає, що довіра та тісний зв’язок в он-лайні можуть виникати досить швидко. Хижаки користуються цією анонімністю, щоб будувати свої взаємовідносини з недосвідченими молодими людьми. Батьки можуть захистити своїх дітей, якщо вони будуть обізнані з ризиками он-лайн-спілкування та цікавитимуться діяльністю своїх дітей у мережі Інтернет. Батькам потрібно бути добре поінформованими, щоб отримати відповіді на свої запитання про те, як діють он-лайн-хижаки, хто ризикує стати їхньою жертвою та як знизити для своєї дитини ризик стати мішенню інформаційних атак.

Як діють он-лайн-хижаки?

Хижаки встановлюють контакт із дітьми шляхом розмов у чат-кімнатах, обміну миттєвими повідомленнями, завдяки електронній пошті або дошкам повідомлень. Багато підлітків користуються он-лайн-форумами підтримки ровесників для розв’язання своїх проблем. Хижаки часто відвідують такі зони в он-лайні для пошуку вразливих жертв. Он-лайн-хижаки намагаються

поступово спокусити своїх жертв, виявляючи по відношенню до них увагу, доброту або навіть пропонуючи подарунки. Як правило, не шкодують ні часу, ні грошей, ні енергії. Вони в курсі найостанніших музичних новинок і все знають про хобі, які цікавлять дітей. Вони вислуховують дітей і співчувають їхнім проблемам, намагаються «послабити комплекси» молодих людей, поступово вводячи у свої розмови сексуальний контекст або показуючи їм відверто сексуальні матеріали. Деякі он-лайн-хижаки намагаються одразу ж втягнути дітей у відверто сексуальні розмови. Цей більш прямолінійний підхід може включати і сексуальне домагання. Хижаки також можуть запрошувати дітей, з якими вони знайомляться в он-лайні, до контакту віч-на-віч.

Гра «Правда чи брехня і чому?»

Я пропоную вам виконати декілька завдань.

Завдання 1. Уважно прослухайте листи. Яку відповідь ви дасте на них? Обґрунтуйте.

Лист 1. Привіт! Мене звати Сашко. Мені 15 років. Я живу в Києві. Шукаю друзів по переписці. Я полюбляю комп'ютерні ігри, читати книги, дивитися телевізор. Я мрію подорожувати. Хочу побувати в Лондоні ....

Лист 2. Привіт! Мене звати С. Я хочу з тобою познайомитися. Мені 30 років. Я живу в Сполучених Штатах Америки. Я маю власну фірму. У мене свій двохповерховий будинок. Я збираюся відвідати Україну. Може ми зустрінемося? Пришли мені свою фотокартку та домашню адресу.

Лист 3.

Наша організація займається збиранням коштів для потерпілих від повені в N. Ми купуємо їжу, теплі речі для тих, хто втратив домівки. Не будьте байдужими до чужого горя! Хто скільки може. Наш рахунок № 123456789.

Вдячні діти Вас ніколи не забудуть.

Дякуємо.

Хто ризикує стати жертвою он-лайн-хижаків?

Юнаки та дівчата є найбільш вразливою категорією, яка знаходиться під загрозою контактів з он-лайн-хижаками. Молодь досліджує свою сексуальність, виходить з-під батьківського контролю й шукає нових стосунків за межами сім'ї. Виходячи в Інтернет під маскою анонімності, вони, скоріш за все, ризикують стати чиїмись жертвами в он-лайні, цілком не розуміючи до кінця можливих наслідків. Молоді люди, які є найбільш вразливими для он-лайнових хижаків, мають наступні риси:

• Вони новачки в он-лайні й незнайомі з «мережевим етикетом».

•Завзяті користувачі комп'ютера.

• Хочуть спробувати щось нове, авантюрне у житті.

• Активно шукають уваги та теплих стосунків.

• Бунтівні.

• Ізольовані або самотні.

• Допитливі.

• Збентежені в плані статевої приналежності.

• Занадто довірливі, яких можна легко ошукати.

• Їх приваблюють субкультури, що існують за межами їхнього контрольованого батьками світу.

Діти вважають, що вони знають про всю небезпеку хижаків, але насправді вони наївні, коли мова йде про он-лайн-стосунки.

Як уберегтися від непроханих відвідувачів?

Є багато людей, які намагаються отримати доступ до чужих комп'ютерів. Проте існують за особи, що утримують цей процес або навіть унеможливлюють його. Найпоширеніші з них — брандмауери, а також антивірусне та антиспамове програмне забезпечення. Велике значення має також дотримання користувачами правил безпеки під час роботи в Інтернеті.

Брандмауери

Взагалі брандмауер - це стіна з вогнестійкого матеріалу, що розташована між будинками й захищає їх від пожежі. Якщо вогонь

вируватиме зовні, така стіна не дозволить йому досягти будинку. У комп'ютерній мережі брандмауером називають програмне забезпечення, яке захищає локальну мережу від небезпек. Брандмауер розташовують між локальною мережею та Інтернетом або між окремими ланками локальної мережі. Він відстежує й аналізує весь потік пакетів із даними, що надходить до нього, і пропускає лише дозволе ні пакети. Таким чином, небезпечний код з Інтернету не може потрапити до локальної мережі.

Антивірусне програмне забезпечення

Найбільшою загрозою для комп'ютерних систем є віруси. Для боротьби з ними можна придбати програмне забезпечення, що називається антивірусним. Воно працюватиме у вашій системі й перевірятиме на вміст вірусів усі файли, які ви отримуєте електронною поштою, завантажуєте з Інтернету, переписуєте на жорсткий диск або запускаєте на виконання з компакт-диска чи дискети.

Більшість виробників антивірусних програм пропонують пробні версії, які можна завантажити на комп'ютер і використовувати протягом певного часу. Пробними версіями можуть бути укомплектовані також нові комп'ютери.

Незалежно від того, яку з антивірусних програм ви виберете, важливо постійно її оновлювати. Зазвичай за певну річну оплату ви може те завантажувати оновлення з сайту виробника. Більшість програм самостійно щоденно підключаються до свого сайту й перевіряють, чи нема там «свіжих» оновлень.

Запобігання зараженню вірусами

Як було зазначено, немає й не може бути сто відсоткової гарантії того, що ви ніколи не підхопите в Інтернеті вірус, не зазнаєте вторгнення чи не отримаєте спам. Певний ризик завжди існує. Для запобігання цьому потрібно використовувати від повідні програмні засоби, завжди керуватися здоровим глуздом та дотримуватися правил безпечної поведінки в Інтернеті. Ось деякі з цих правил:

- На комп'ютері завжди має функціонувати антивірусне програмне забезпечення. Стежте за його актуальністю. Налаштуйте програму в такий спосіб, щоб вона автоматично сканувала систему, коли ви не працюєте, скажімо, по неділях чи вночі.
- Не відкривайте додані файли, які надходять разом із повідомленнями електронної пошти, якщо ви не впевнені, що вони містять саме ті дані, на які ви чекаєте.
- Використовуйте лише те програмне забезпечення, яке надійшло з перевірених джерел.
- Своєчасно оновлюйте операційну систему.

Листівка для кожного учня. (Правила Інтернет-БЕЗПЕКИ І Інтернет-ЕТИКИ та роботи за комп'ютером).

Правила Інтернет-БЕЗПЕКИ І Інтернет-ЕТИКИ

1. Ніколи не давайте приватної інформації про себе (прізвище, номер телефону, адресу, номер школи) без дозволу батьків.
2. Якщо хтось говорить вам, надсилає вам, або ви самі віднайшли у мережі щось, що бентежить вас, не намагайтеся розібратися в цьому самостійно. Зверніться до батьків або вчителів - вони знають, що треба робити.
3. Зустрічі у реальному житті із знайомими по Інтернет-спілкуванню не є дуже гарною ідеєю, оскільки люди можуть бути дуже різними у електронному спілкуванні і при реальній зустрічі. Якщо ж ви все ж хочете зустрітися з ними, повідомте про це батьків, і нехай вони підуть на першу зустріч разом з вами
4. Не відкривайте листи електронної пошти, файли або Web-сторінки, отримані від людей, яких ви реально не знаєте або не довіряєте.
5. Нікому не давайте свій пароль, за виключенням дорослих вашої родини.

6. Завжди дотримуйтесь сімейних правил Інтернет-безпеки: вони розроблені для того, щоб ви почували себе комфортно і безпечно у мережі.

7. Ніколи не робіть того, що може коштувати грошей вашій родині, окрім випадків, коли поруч з вами батьки.

8. Завжди будьте ввічливими у електронному листуванні, і ваші кореспонденти будуть ввічливими з вами.

9. У електронних листах не застосовуйте текст, набраний у ВЕРХНЬОМУ РЕГІСТРІ - це сприймається у мережі як крик, і може прикро вразити вашого співрозмовника.

10. Не надсилайте у листі інформації великого обсягу (картинки, фотографії тощо) без попередньої домовленості з вашим співрозмовником.

11. Не розсилайте листи з будь-якою інформацією незнайомим людям без їхнього прохання - це сприймається як "спам", і звичайно засмучує користувачів мережі

12. Завжди поводьтеся у мережі так, як би ви хотіли, щоб поводилися з вами!

Правила безпеки при роботі з комп'ютером

1. Комп'ютер потрібно розташувати в кутку або задньою стінкою до стіни. Забезпечити максимальну фокусну відстань. Комп'ютер повинен бути встановлений так, щоб, відірвавши очі від монітора, враз можна було побачити найвіддаленіший предмет у кімнаті. При розміщенні комп'ютера в кутку кімнати слід встановити на верхній частині монітора або на столі велике дзеркало. Тоді ви бачитимете далекі предмети, що знаходяться за вашою спиною.

2. Прослідкувати за відсутністю відблисків. При їх наявності: змініть кут нахилу екрана; перемістіть в кімнаті усі предмети, які відблискують на екрані; спробуйте опустити освітлювальні прилади або електролампочки нижче; закрийте люмінесцентні лампи решітками; поверніть екран монітору так, щоб він був перпендикулярним до приладів освітлення; відрегулюйте освітлення екрана ручками яскравості й контрастності.

3. Змонтувати правильне і раціональне освітлення робочого місця. Найкращим варіантом верхнього освітлення робочої кімнати може бути устаткування з регульованим світловим потоком і, бажано, спрямованим безпосередньо на стелю.

4. Монітор має бути розміщений дещо нижче, так, щоб ви дивилися на нього зверху вниз під кутом 15-30° до горизонту або лінії погляду. Це допоможе значно зменшити напругу, очі будуть напівприкриті повіками і менше втомлюватимуться. Відстань від монітора до очей має дорівнювати приблизно довжині витягнутої руки (не менш ніж 45-60 см від екрана монітора, до того ж на 15-20 см вище його центру). Не можна працювати з поставленою на максимум яскравістю й контрастністю.

5. Стілець обов'язково має бути зі спинкою. Комп'ютер потрібно розмістити не менш ніж за 50-70 см від людини (що далі, то краще). Сидіти потрібно прямо або злегка нахилившись уперед, із невеликим нахилом голови, та спираючись на 2/3-3/4 довжини стегна. Між корпусом тіла і краєм столу зберігається вільний простір не менш ніж 5 см. Руки вільно лежать на столі. Ноги зігнуті в тазостегновому і колінному суглобах під прямим кутом і розташовані під столом на підставці.

6. Пальці повинні бути трохи нижче рівня зап'ястя, а воно — нижче рівня ліктів. Тоді пальці володітимуть найбільшою свободою руху.

7. Плечі опущені й розслаблені, щоб і руки могли бути розслаблені.

8. У приміщенні, де працює комп'ютер, необхідне щоденне вологе прибирання. Тому підлогу в кімнаті не треба накривати килимом.

9. До і після роботи на комп'ютері слід протирати екран спеціальними серветками.

10. Не забувайте частіше провітрювати кімнату. Акваріум або інші ємності з водою збільшують вологість повітря.

11. Для того щоб очі не втомлювалися і зір не погіршувався, необхідно: кліпати очима кожні 3-5 с; дивитися не тільки на екран, слід відводити від нього погляд на оточуючі предмети і рухомі об'єкти; давати

короткочасний відпочинок очам (також тілу, кінцівкам) — кожні 2-3 хв кидати короткий погляд на далекий предмет або в дзеркало; робити короткі, 2-3-хвилинні перерви на відпочинок через кожні 20 хв роботи. І зазвичай, не забувати про загальнофізичну гімнастику, яка дасть можливість уникнути застою крові в судинах, її загущення й негативних наслідків гіподинамії. Під час робочого дня треба робити регулярні перерви для легких фізичних вправ.

Увага! Фахівці радять розташовуватися подалі від екрана, користуватися тільки спеціальними зручними меблями, проводити розслаблюючі для очей зарядки, робити короткі перерви у роботі. Поглинання електромагнітного випромінювання мозком проходить нерівномірно і призводить до різних структурних змін нейроклітин у зоні поглинання, а під дією торсійної компоненти утворює різноманітну клінічну картину (хвороби Паркінсона, Альцгеймера і т. д.). У Швейцарії, приміром, законодавством про роботу жінкам дітородного віку робота на ПК більше чотирьох годин на добу заборонена. У Німеччині робота на ПК входить у перелік десятьох найбільш шкідливих для здоров'я людини. У багатьох країнах заборонено використання систем мобільного зв'язку у лікарнях, дитячих установах.

Достовірно встановлено, що на користувача ПК впливає цілий комплекс факторів, прихованих від наших звичайних людських органів відчуттів, — це ультрафіолетове та ультрачервоне, рентгенівське випромінювання — негативна дія яких розвивається в організмі людини поступово і в міру накопичення. Тому захворювання можуть проявлятися лише після декількох місяців, а то й років роботи з ПК, коли вже буде надто важко встановити їхні причини. Всесвітня організація охорони здоров'я (ВООЗ) розглядає роботу з ПК як фактор постійно діючого стресу. Робоча група ВООЗ з гігієнічних аспектів користування виділила порушення стану здоров'я при користуванні пристроями, що мають електромагнітне випромінювання.

Найсерйозніші з них такі:

- онкологічні захворювання (вірогідність їх зростає пропорційно тривалості впливу електромагнітного випромінювання на організм людини);

- гноблення репродуктивної системи (імпотенція, зниження лібідо, порушення менструального циклу, уповільнення статевого дозрівання, зниження здатності до запліднення і т. п);

- несприятливий хід вагітності (при роботі з ПК тривалістю більше 20 годин у тиждень, у жінок вірогідність викиднів зростає у 2,7 р., а народження дітей з уродженими недоліками — в 2,3 р., ніж у контрольних групах;

- вірогідність порушення ходу вагітності зростає в 1,3 р. при тривалості роботи під впливом електромагнітних випромінювачів більше 4 годин на тиждень.

- порушення психоемоційного стану (стресовий синдром, агресивність, дратівливість, погіршення зору і хвороби органів зору);

- лейкемія (рак крові) у людей, що в силу своєї професії постійно контактують з електромагнітним випромінюванням.

Висновок. Отже, спілкування, одержання інформації у становленні особистості людини посідає одне з найважливіших місць. Але завжди слід пам'ятати, що найважливіше для людини є її здоров'я і фізичне, і психічне, і соціальне.