ЗАХИСТ ІНФОРМАЦІЇ

Є. Ю. Мацо, с. Зарічево, Перечинський р-н, Закарпатська обл.

Цілі:

навчальна: сформувати в учнів поняття безпеки і необхідності захисту інформації, визначити основні напрями;

розвивальна: розвивати пізнавальний інтерес, навички самостійної роботи і роботи в колективі, уміння застосовувати знання, навички в різних ситуаціях;

виховна: виховувати культуру мовлення, працелюбність, прищеплювати бажання мати глибокі і якісні знання, виховувати зібраність, організованість, відповідальність, уміння співпрацювати в колективі.

Форма проведення уроку: ігрові технології — віртуальний форум.

Наочність та обладнання: мультимедійне забезпечення, презентаційний матеріал, роздавальний матеріал.

Хто володіє інформацією,
той володіє світом.

ХІД УРОКУ

І. ОРГАНІЗАЦІЙНИЙ ЕТАП (7 ХВ)

Учитель. Усім нам добре відомий такий вислів: «Хто володіє інформацією, той володіє світом». Ким би ви не стали в майбутньому, ви повинні пам'ятати: наше суспільство перетворилося з індустріального на інформаційне. Ви є свідками й учасниками бурхливого розвитку інформаційних технологій, який, у свою чергу, потребує захисту інформації. Для захисту інформації потрібен не лише професійний, а й культурний рівень, який визначається розумінням інформаційних процесів і вмінням користуватися новітніми технологіями.

Кожен з нас має інформацію, яка є в певній мірі важливою чи секретною: наприклад, це номери телефонів чи смс-повідомлення в мобільних телефонах, пін-коди банківських карток, файли на комп'ютері та ін.

Крім вищенаведеного є багато іншої інформації: проекти великих компаній, електронні бази даних, електронні бібліотеки, банківська система тощо, яка також потребує захисту.

На законодавчому рівні інформація, інтелектуальна власність захищається законом (стаття 361-1 Кримінального кодексу про злочини у сфері використання ЕОМ).

До цього часу ми вивчали будову і принцип роботи комп'ютера, навчилися створювати та зберігати файли, вміємо користуватися периферійними пристроями, використовувати різні програмні продукти, а сьогодні ми ознайомимося з питаннями захисту інформації.

Тема сьогоднішнього уроку — «Захист інформації» — надзвичайно актуальна. Ми розглянемо, у яких випадках і як потрібно захищати інформацію, від кого чи чого берегтися, наслідки пошкодження чи зникнення інформації.

ОРГАНІЗАЦІЯ РОБОТИ ФОРУМУ (3 ХВ)

Учитель. Урок проведемо у вигляді віртуального форуму, використовуючи ваш власний досвід, домашнє завдання та підготовку до проведення форуму.

! *Форум* — інтернет-ресурс, популярний вид спілкування в інтернеті.

Для проведення форуму ознайомимося з правилами ведення форуму.

! Правила ведення форуму

1. Користувачем цього форуму є кожен учень, зарахований до групи _____.
2. За порядком на форумі стежать адміністратори та модератори.
3. Уся інформація наведена для ознайомлення та навчальних цілей.
4. Заборонено використовувати ненормативну лексику, грубі вирази.
5. Заборонено проявляти ворожість до співбесідника, ображати його як-небудь.
6. Усі інші присутні на нашому форумі і ті, хто ввійшов до системи як гість, не можуть брати участі в обговоренні.
7. Якщо гостям сподобався наш форум, вони можуть залишити своє повідомлення на сайті Перечинського професійного ліцею.

Визначення функцій модератора та адміністратора

(*Адміністратор* — викладач, який у певний момент часу рекомендує форумчанам записувати в зошити інформацію (наприклад, зі слайдів).

Модератор — учень, який стажить за роботою форуму, за дотриманням правил та веде облік повідомлень від кожного учасника.)

Для оголошення повідомлень використовують картки з написами «Повідомлення» і «Цитувати».

Оголошення критеріїв оцінювання повідомлень.

Авторизація учасників форуму у віртуальній мережі.

Усі учасники форуму прикріплюють підготовлені картки — ніки.

II. ПРОВЕДЕННЯ ФОРУМУ (25 ХВ)

Під час проведення форуму застосовують випереджувальне навчання, знання, вміння, навички самостійної роботи учнів та їх власний досвід роботи з інформаційними технологіями.

Форум роботу розпочав. Чекаємо на перше повідомлення…

Повідомлення 1

На мою думку, для розкриття цієї теми в першу чергу потрібно обговорити комп'ютерні віруси, адже це найбільша проблема захисту інформації.

Повідомлення 2

Правильно. Я часто чую, що комп'ютерний вірус створює серйозну небезпеку, і в мене виникає запитання: хто і навіщо створює комп'ютерні віруси?

Повідомлення 3

Комп'ютерний вірус — це спеціально створена програма-паразит, яка може «приписувати» себе до інших програм, тобто «заражати» їх, створювати свої копії і впроваджувати їх у файли, документи, системні ділянки комп'ютера тощо, а також виконувати різні небажані дії на комп'ютері. Тут і є відповідь.

Повідомлення 4

Термін «комп'ютерний вірус» з'явився 1984 року на сьомій конференції з безпеки інформації. Офіційно його автором вважають працівника Лехайського університету США Ф. Коена.

! *Комп'ютерний вірус* — (англ. computer virus) — комп'ютерна програма для заподіяння шкоди користувачеві ПК: крадіжки даних, зниження працездатності комп'ютера тощо.

Повідомлення 5

Чимало знайомих стверджують, що комп'ютерні віруси — це одна з найбільших економічних бід, що відбуваються із сучасними компаніями. Вони обходяться набагато дорожче, ніж пожежі, повені і крадіжки. Один поширений через інтернет вірус може заподіяти мільярдних збитків, виражених у втраті продуктивності, пошкодженні устаткування й у зірваних ділових зустрічах.

Повідомлення 6

Комп'ютерних вірусів на сьогоднішній день дуже багато — декілька тисяч. Їх класифікують за різними ознаками:

- за середовищем існування;
- за способом зараження;
- за деструктивними можливостями;
- за особливостями алгоритму дій.

Кожна з цих ознак ще підрозділяється. Крім того, існують ще й троянські програми, шкідливе програмне забезпечення, спам, фішинг. Але наведену вище інформацію не можна вважати повною, оскільки прогрес не стоїть на місці, з'являються нові інтелектуальні пристрої і відповідно віруси, які працюють на них. Наприклад, мій смартфон теж уразив вірус. Я втратив інформацію.

На закінчення скажу, що вся ця єресь забирає у нас гроші, нервові клітини і переслідує головну мету — нашкодити.

Деякі типи вірусів

Файлові — заражають файли *.exe, *.com.

Завантажувальні — заражають завантажувальні сектори дисків.

Макровіруси — заражають документи з макросами (*.doc, *xls, *mdb).

! *Поліморфні* — за кожного нового зараження змінюють свій код.

Мережні віруси — розповсюджуються через комп'ютерні мережі.

Черв'яки — розповсюджуються через електронну пошту.

«Троянські коні» («трояни») — програми, які дозволяють одержати віддалене керування комп'ютером через інтернет, у тому числі передавати паролі, організовувати масові атаки на сайти.

Повідомлення 7

Втрата інформації — серйозна проблема. Адже «Хто володіє інформацією, той володіє світом».

Повідомлення 8

Правильно. Вірус ви підчепите безкоштовно, а антивірусну програму потрібно купувати.

Повідомлення 9

Вчитися, вчитися, і ще раз учитися, і ще раз учитися, і ще раз учитися, і ще раз учитися, і....

(Комп'ютерний вірус)

Повідомлення 10

Переважна більшість вірусів і троянських програм у минулому створювалася студентами і школярами, які тільки-но вивчили мову програмування, хотіли спробувати свої сили, тобто самоствердживалися їх автори. Вони часто на веб-ресурсах дають докладні рекомендації щодо методів проникнення в систему. Але ставши старшими і досвідченішими, вони потрапляють у небезпечну групу «професійні віруси». Наступна сходинка вірусотворців — «дослідники». Вони пишуть віруси не заради самих вірусів, а швидше заради дослідження потенціалу «комп'ютерної фауни», активно пропагують свої ідеї через численні інтернет-ресурси. Але коли такі «дослідницькі віруси» потрапляють до рук професіоналів з попередньої групи… начувайтеся.

Повідомлення 11

З появою платних інтернет-сервісів збільшується кількість охочих отримати доступ до мережі за чужий рахунок, тобто за допомогою крадіжки чийогось логіна і пароля шляхом застосування спеціально створених троянських програм. «Дрібні злодюжки» крадуть реєстраційні дані, ключові файли різних програмних продуктів, ігор на користь свого «господаря». Вони пропонують піратські (неліцензійні) версії програмних продуктів. Але спостерігається здешевлення інтернет-сервісів…

Повідомлення 12

Найнебезпечніша група вірусотворців — хакери-одинаки або групи хакерів, які усвідомлено створюють шкідливі програми з єдиною метою: отримати чужі гроші (рекламуючи що-небуть або просто крадучи їх), ресурси зараженого комп'ютера (знову-таки, заради грошей, для обслуговування спам-бізнесу або організації DOS-атак з метою подальшого шантажу і вимагання викупу за припинення атак) — це кримінальний бізнес.

Повідомлення 13

А я думав, що тільки створюючи антивірусні програми можна заробити гроші, а тут і віруси можуть роздобути непогану копійчину.

Повідомлення 14

Так, так. Але не забуваймо про кримінальну відповідальність, у будь-якому випадку вирахують, і не таких хакерів вираховували. Краще все-таки вчитися і створювати антивірусні програми. До речі, є стаття 361-1 Кримінального кодексу про злочини у сфері використання ЕОМ, де за таке карають позбавленням волі на 3–5 років.

Повідомлення 15

А якщо я постійно перевіряю дискети і не користуюся мережею інтернет, то мене зараження може обійти?

Повідомлення 16

Перевірена дискета чи інший носій інформації ще не гарантує відсутність вірусу.

Повідомлення 17

У такому випадку звідки мені знати, є у мене вірус чи нема?

Повідомлення 18

Є ряд симптомів, що свідчать про зараження комп'ютера: довільний запуск програм, відкриття і закриття лотка CD-ROM пристрою, подача звукових сигналів, непередбачені повідомлення, часті зависання і збої в роботі комп'ютера, зникнення файлів чи папок, спотворення інформації, вікна програм неможливо закрити, уповільнення роботи тощо. Якщо у вас подібні симптоми — вам потрібна лікарська допомога.

Шкідливі дії:

- звукові і візуальні ефекти;
- імітація збоїв ОС і апаратури;
- самовільне перезавантаження комп'ютера;
- розвалювання файлової системи;
- знищення інформації або її спотворення;
- передавання секретних даних через інтернет.

Ознаки:

- сповільнення роботи комп'ютера;
- перезавантаження або зависання комп'ютера;
- неправильна робота ОС або прикладних програм;
- зміна довжини файла;
- поява нових файлів;
- зменшення об'єму оперативної пам'яті.

Повідомлення 19

Для того щоб уберегтися від зараження, ми повинні знати, що основними джерелами вірусів є мережа інтернет, електронна пошта, піратські копії програм, комп'ютери в локальній мережі. Тобто те, без чого ми вже не обходимося майже щодня.

Антивірусна програма (антивірус) — програма для знаходження і, можливо, лікування програм, що заражені комп'ютерним вірусом, а також, можливо, для запобігання зараження файла вірусом.

Повідомлення 20

Ну що ж ви так розплакалися: комп'ютерні віруси, небезпека, втрата всього. Поставте антивірусну програму і не знайте жодних проблем.

Повідомлення 21

Правильно, але я раджу ставити ліцензійні, оскільки вони надійніші за піратські і мають можливість постійно оновлюватися через мережу інтернет, а платите тільки один раз. А неліцензійні версії постійний головний біль: то термін вийшов, то ще щось не так, то ключ коштує певну суму. Вірусна база поновлюється майже щодня, а то й частіше, і відповідно постійного оновлення потребують антивірусні програми.

Повідомлення 22

В принципі в мережі інтернет можна знайти безкоштовно антивірусні програми з різними термінами дії.

Повідомлення 23

А я практикую після закінчення терміну дії антивірусної програми встановлювати нову, так і виходжу з цієї ситуації. Морока, але мене такий варіант влаштовує, мені цікаво.

Повідомлення 24

А яку антивірусну програму порекомендуєте?

Антивірусні програми

- Антивірус Касперського Personal — «Лабораторії Касперського».
- DrWeb — «Диалогнаука».
- Norton Antivirus — «Symantec».
- VirusScan — «McAfee».
- eSafe Desktop — «Aladdin Knowledge Systems» та ін.

Типи антивірусів:

- *Програми-сканери* — аналізують програми і файли з макросами на наявність послідовності команд, що характерна для якого-небудь вірусу.
- *Програми-ревізори* запам'ятовують первісний (незаражений) стан файлів і папок і вважають їх еталонними.

Програми-евристичні аналізатори аналізують окремі дії і ознаки, характерні для програм-вірусів.

Повідомлення 25

Антивірус Касперського.

Повідомлення 26

У Касперському трохи розчарований тому, що він забирає багато ресурсів в ОС і сповільнює роботу фактично всього. DrWeb — непоганий варіант, але виникають проблеми з ліцензію, так само як і в Nod32.

Повідомлення 27

У мене в комп'ютері 256 Мб оперативки і Касперський 7.0 працює нормально, і комп'ютер практично не зависає. Та й віруси він виявляє нормально. На комп'ютери з 128 Мб оперативної пам'яті його звісно ставити не варто. А в друга 1,5 Гб ОЗУ, то взагалі жодних проблем. Користуюсь поки що ним, зручнішого не знайшов.

Повідомлення 28

Мені подобається Avira AntiVir® PersonalEdition Classic. У безкоштовної версії є низка обмежень, але для роботи користувача достатньо. На рахунок Avast були випадки, коли він досить злісних «троянів» просто не помічав. За можливості можна під час роботи в інтернеті використовувати Linux, тоді проблеми з вірусами фактично зникнуть.

Повідомлення 29

Уже давно користуюсь DrWeb. Маю останню версію з ключем. Також можу оновлювати бази щодня так, щоб не банився ключ.

Повідомлення 30

ESET NOD32 порівняно з іншими антивірусними системами превентивно (тобто багаторівнево) виявляє і блокує всі відомі раніше і більшість невідомих вірусів, рекламних, троянських, фішинг-програм, черв'яків, руткітів та інші інтернет-загрози. Має функції антишпигунського ПЗ, антиспама та брандмауера, мінімізує загрозу зараження новим вірусом у проміжку між його появою та оновленням баз.

Повідомлення 31

Отже, я роблю для себе такий висновок: кожна антивірусна програма має свої переваги і недоліки. Все залежить від того, який у мене комп'ютер, якого я рівня користувач. Я напевно куплю собі програму, яка попадеться, можливо, подивлюся ще і на ціну, а там буде видно…

Повідомлення 32

А я можу скинути ссилку рейтингів найкращих антивірусних програм за 2012 рік. В інтернеті натрапив.

Повідомлення 33

Розмова в родині комп'ютерщиків:

— Тату, а який надійніший засіб вилікувати Windows?

— Синку, надійніший засіб вилікувати Windows — це FORMAT C:.

Повідомлення 34

Щоб цей жарт не трапився з вами, я порекомендувала б стежити за новинками на сайтах антивірусних компаній і прислухатися до порад фахівців з інформаційної безпеки, адже можливо деякі недоліки, які виявили ви або ваші друзі, є просто наслідками ваших некоректних дій.

Повідомлення 35

Хочу розповісти ситуацію, яка трапилася зі мною. Була в мене, не пам'ятаю яка, антивірусна програма, я її видалив неправильно (тобто тільки ярлик) і встановив іншу. Комп'ютер завис надовго і завантажувався півдня. Друзі сказали мені, що в одному комп'ютері одночасно не можна встановлювати дві і більше антивірусних програм, оскільки вони сприймають одна одну як вірус. Не повторіть моєї помилки.

Повідомлення 36

Форумчани, я думаю, що ми недооцінили антивірус Касперського, оскільки він дозволяє захистити комп'ютер від мережних хакерських атак з локальної мережі або інтернету. Виявлення хакерських атак виконується на основі баз відомих на поточний час атак. Ці бази оновлюються і встановлюються разом з антивірусними. Захист від мережних атак запускається одночасно з антивірусом та відстежує всі мережні з'єднання і перевіряє всі дані, що приймаються через мережу, незалежно від джерела. Як тільки буде вчинена спроба атакувати ваш комп'ютер, вона буде блокована. На екран буде виведено повідомлення, що містить інформацію про вид атаки, IP-адресу атакуючого комп'ютера і локальний порт.

Повідомлення 37

Крім хакерських атак комп'ютер потрібно захищати від різних інтернет-загроз, тобто спроб порушувати працездатність комп'ютерних систем, спроб злому захисту систем, використання і розповсюдження програм, що порушують працездатність.

Повідомлення 38

Компанія Eset опублікувала список найпоширеніших інтернет-загроз, виявлених фахівцями вірусної лабораторії Eset у жовтні 2009 року. Світовий рейтинг шкідливих програм очолив черв'як Conficker. Загальний відсоток зараження склав 8,85%. На другому місці світового вірусного рейтингу знаходяться загрози, які використовують файл Autorun.inf. Загальний відсоток зараження складає 7,73%.

Повідомлення 39

Через прихований характер зараження багато користувачів недостатньо серйозно ставляться до власної інтернет-безпеки. 40% респондентів упевнені, що їхній робочий комп'ютер краще захищений від спама, шпигунських програм і фішинга порівняно з домашнім комп'ютером. У результаті ці користувачі з більшою імовірністю заходять по підозрілих лінках, коли знаходяться на робочому місці (17% респондентів). За матеріалами інтернет-сайтів.

Повідомлення 40

Компанія Panda Security опублікувала рейтинг найнебезпечніших інтернет-загроз за останні 20 років. Рівень небезпеки загрози визначали залежно від рівня відомості та пошкоджень, які спричинив вірус чи троян.

До першої п'ятірки інтернет-загроз увійшли:

- «П'ятниця 13», або «Єрусалим» (з'явилася в Ізраїлі 1988 р. на 40-ву річницю Ізраїля. У п'ятницю, 13 числа вона видаляла всі встановлені на комп'ютері програми);
- «Тюремный узник». Вірус, який з'явився 1993 року, активувався 5 січня і відображав на екрані монітора тюремні ґрати;
- «Каскад» — після зараження букви на екрані монітора перетворювалися на падаючий каскад;
- CIH, або «Чорнобиль» — вірус, який 1998 р. за один тиждень зумів заразити тисячі комп'ютерів;
- «Мелисса» — вірус, який 1999 року вперше використаний соціальною інженерією для розповсюдження. Користувачі отримували такі повідомлення: «Документ, который Вы запрашивали… никому его не показывайте ;-)».

Повідомлення 41

Ми можемо захиститися від інтернет-загроз, використовуючи спеціальні програми — *брандмауери*. *Брандмауер* — це програмний засіб, який використовують для настроювання обмежень, що регулюють обмін даними між інтернетом і окремим комп'ютером чи локальною мережею. Операційна система Windows має свій центр забезпечення безпеки — вбудований брандмауер.

Повідомлення 42

Брандмауер обмежує інформацію, яка надходить на комп'ютер від інших комп'ютерів, дозволяє краще контролювати дані на комп'ютері, забезпечуючи тим самим лінію захисту від людей чи програм, включаючи віруси і черв'яки, які несанкціоновано підключаються. Можна вважати брандмауер митним контролем, на якому перевіряється інформація (трафік).

Брандмауер — це програмний засіб для настроювання обмежень, що регулюють обмін даними між інтернетом та окремим комп'ютером чи локальною мережею.

Повідомлення 43

Не обов'язково використовувати саме брандмауер Windows — можна встановити інший. У такому випадку треба відключити брандмауер Windows. Оцініть можливості інших, а потім вирішуйте, який краще вам підходить.

Повідомлення 44

Коли до комп'ютера робиться спроба підключення з інтернету або локальної мережі, тобто «непередбачені запити», брандмауер блокує підключення і видає запит користувачеві про блокування або дозвіл підключення. Якщо користувач дозволяє підключення, то брандмауер створює виняток, щоб надалі не турбувати запитами для цієї програми.

Повідомлення 45

Звісно, добре мати останнє оновлення антивірусної програми, потужний брандмауер, а я запропоную вам час від часу робити резервне копіювання вашої цінної інформації, і бажано на зовнішні носії. Наприклад, резервування інформації на окремому жорсткому диску того ж комп'ютера створює тільки ілюзію безпеки. Окремо потрібно зберігати різні реєстраційні дані та паролі, причому можна і на папері, але в надійному місці чи сейфі керівника.

Повідомлення 46

Є ще один досить новий і надійний прийом зберігання інформації (не конфіденційної) — це зберігання у веб-папках на віддалених серверах в інтернеті. Є служби, які надають безкоштовно простір (до декількох гігабайтів) для зберігання даних користувача.

Повідомлення 47

Десь чув про несанкціонований доступ до інформації, і що від таких речей також потрібно захищатися. В матеріалах з Вікіпедії — вільної енциклопедії — знайшов, що несанкціонований доступ до інформації — доступ до інформації з порушенням посадових повноважень працівника, доступ до закритої для публічного доступу інформації з боку осіб, котрі не мають дозволу на доступ до цієї інформації. Також іноді несанкціонованим доступом називають одержання доступу до інформації особою, яка має право на доступ до цієї інформації в обсязі, що перевищує необхідний для виконання службових обов'язків.

Причини несанкціонованого доступу до інформації:

- помилки конфігурації (прав доступу, брандмауерів, обмежень на масовість запитів до баз даних);
- слабка захищеність засобів авторизації (розкрадання паролів, смарт-карт; фізичний доступ до устаткування, що погано охороняється; доступ до незаблокованих робочих місць працівник під час їх відсутності);
- помилки в програмному забезпеченні;
- зловживання службовими повноваженнями (викрадання резервних копій, копіювання інформації на зовнішні носії за права доступу до інформації);
- прослуховування каналів зв'язку під час використання незахищених з'єднань усередині ЛОМ;
- використання клавіатурних шпигунів, вірусів і троянів на комп'ютерах працівників.

Повідомлення 48

Я вважаю, що і цю проблему можна розв'язати. На робочому місці або на домашньому комп'ютері за наявності декількох користувачів інформацію можна захистити паролем. У налаштуваннях панелі керування є можливість створити обліковий запис користувача, тобто свій пароль входу в систему. Це ми бачимо на наших учнівських комп'ютерах: режим учня і режим вчителя. У нашому випадку ми кожен можемо створити власний обліковий запис. Дехто уже створив…

Повідомлення 49

Це також хороший варіант після антивірусних програм для захисту своєї інформації від колег чи брата/сестри.

Повідомлення 50

Але вчитель має доступ до нашого режиму і бачить наші творіння.

Повідомлення 51

Звісно бачить, тому що на учнівських комп'ютерах створюються навчальні документи, а не секретні.

І у вчителя права адміністратора, а тут іде мова про колег чи родичів.

Повідомлення 52

Форумчани! Наші ніки також певним чином захищають інформацію про кожного з нас. І свою електронну пошту ми також захищаємо паролем. І свої папки на комп'ютері. Ми зашифрувалися.

Повідомлення 53

Але я все-таки не зрозумів, що таке мережні атаки. Поясніть простіше.

Повідомлення 54

Наприклад, для порушення працездатності серверу використовують направлену атаку TCP-запитів. Атака полягає в постійній передачі на об'єкт атаки фальшивих запитів на створення з'єднання від імені будь-якого хосту. Завершенням атаки може бути і відмова в обслуговуванні і зависання системи. Це пов'язано з тим, що атакована система має зберігати в пам'яті отриману інформацію і відповісти на кожен запит, що приводить до переповнення черги запитів. Або інший варіант — отримавши певну кількість фальшивих запитів на підключення, система відповість на них і буде очікувати (наприклад, 10 хвилин) на відповіді від неіснуючих хостів, не приймаючи нові запити на з'єднання.

Повідомлення 55

DOS-атаки можуть бути настільки потужними, що зовнішні канали не витримують подібного навантаження і стають цілком зайняті запитами, що надходять, системи зависають. Але Україна істотно краще включена у світовий інтернет, у нас багато каналів, і вони різноманітні.

III. УЗАГАЛЬНЕННЯ ЗНАНЬ ТА ПІДСУМКИ УРОКУ (6 ХВ)

Учитель. На цьому можемо припинити роботу форуму, оскільки основні питання ми розглянули. Хоч повідомлень було багато, але не можемо стверджувати, що ця тема повністю розкрита.

Я дуже вдячна вам за хорошу підготовку до уроку.

Сьогодні ми були учасниками нехай і віртуального, але форуму. Що ви взяли із сьогоднішнього заняття-форуму для себе? (*Відповіді учнів*.)

! Висновки

В обчислювальній техніці поняття безпеки і захисту інформації є досить широким. Воно передбачає:

- надійність роботи комп'ютера;
- збереження цінних даних;
- захист інформації від внесення в неї змін не уповноваженими особами;
- захист від комп'ютерних вірусів, мережних атак, інтернет-загроз;
- збереження таємниці листування під час електронного листування;
- законодавча база.

Ви прийдете додому, до своїх улюбленців, до яких звертаєтеся майже щодня. Що ви, вивчивши сьогоднішню тему, зробите в першу чергу? (*Відповіді учнів*.)

ФРОНТАЛЬНЕ ОПИТУВАННЯ (3 ХВ)

1. Що таке комп'ютерний вірус?
2. Хто і чому створює шкідливі програми?
3. Що таке антивірусна програма?
4. Виберіть правильну відповідь та доповніть перелік.

Для захисту інформації використовують: антивіруси, спам, брандмауери, фішинг, троянські програми, резервні копії та ін.

Учні дають відповіді в письмовій формі на роздавальних картках.

Модератор повідомляє присутнім кількість повідомлень від кожного учасника. Учитель обґрунтовує оцінки, враховуючи усні відповіді та письмові повідомлення.

IV. ДОМАШНЄ ЗАВДАННЯ

Література

1. *Баженов В. А., Зайчик В. О., Лізунов П. П., Шишов О. В.* Інформаційні технології в будівництві : Підручник. — К. : АРКА, 2003.
2. *Глинський Я. М.* Інформатика: 8–11 класи. : Навч. посібник для загальноосвітніх навчальних закладів: У 2-х кн. — Кн. 2. Інформаційні технології. 3-тє вид. — Львів : Деол, СПД Глинський, 2003.
3. *Глинський Я. М.* Практикум з інформатики : навч. посібник. Самовчитель — 11-те вид. — Львів : СПД Глинський, 2008.
4. *Гуржій А. М., Поворозник Н. І., Самсонов В. В.* Інформатика та інформаційні технології. — Х. : Компанія СМІТ, 2003.
5. *Редько М. М.* Інформатика та комп'ютерна техніка : навчально-методичний посібник. — Вінниця : Нова книга, 2007.
6. *Шестопалов Є. А.* Інформатика 10–11 клас. — Шепетівка : Аспект, 1998.

■