УДК 37.016:004

ЗМІСТ І МЕТОДИКА ВИВЧЕННЯ ОСНОВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У 7 КЛАСІ

Руденко Віктор Дмитрович,

провідний науковий співробітник Інституту педагогіки НАПН України, кандидат педагогічних наук, доцент, csf221@rambler.ru..

Анотація. Обгрунтовано зміст і запропоновано методику вивчення основ інформаційної безпеки у сьомому класі, наведені правила, яких слід дотримуватися для надійної роботи комп'ютера і збереження даних, описані основні можливості програми avast!, запропоновано методику роботи в середовищі avast! Free.

Ключовіслова: інформаційна безпека, комп'ютерна безпека, комп'ютерні віруси, шкідливі програми, антивіруси, avast!.

У сьомому класі навчальною програмою [1] передбачено вивчення теми «Основи інформаційної безпеки», на яку відведено дві години. Це нова, досить складна тема. У попередніх програмах вона зводилася до розгляду вірусів і антивірусних програм і вивчалася у 9-му або 10-му класах. Наприклад, у підручнику для 9-го класу [2] описана тема «Антивірусні засоби», а у навчальному посібнику для 8–11-их класів [3] — тема «Віруси й антивірусні програми».

Однак, інформаційна безпека — це не лише захист комп'ютера від вірусів. Інформаційна безпека — це велике за обсягом поняття, для якого так само як і для інформації, не існує і не може існувати однозначного тлумачення. Вонозастосовується в багатьох сферах: інформаційна безпека держави, суспільства, корпорації, особистості, банківської автоматизованої системи, комп'ютерної системи тощо. Актуальність забезпечення інформаційної безпеки на всіх рівнях з кожним роком зростає. Це обумовлено багатьма факторами, зокрема: процесами глобалізації, що відбуваються у світі, швидким зростанням обсягів інформації (в останні роки вони зростають удвічі кожні 2–3 роки), бурхливим розвитком супутникових телекомунікацій, комп'ютерних мереж тощо.

Термін інформаційна безпека виник лише наприкінці 20-го століття у зв'язку з бурхливим розвитком інформаційно-комунікаційних технологій. Але проблема інформаційної безпеки, зокрема, проблема надійного збереження інформації, її конфіденційності, державної таємниці з давнини хвилювала людство. В останні десятиліття ця проблема набула особливого значення у зв'язку зі зростанням ролі й значущості інформації і знань. Інформація стала таким же стратегічним продуктом, як надра й енергія. Відоме речення «Хто володіє інформацією, той володіє світом» є актуальним і в наші дні.

Інформаційна безпека на кожному рівні регулюється нормативно-правовими актами, зокрема: Конституцією і законами країни, міжнародними стандартами (ISO/IEC), державними стандартами (ДСТУ, ГОСТ), галузевими стандартами та іншими. Приклади таких актів в України: закони «Про інформації», «Про захист персональних даних», «Про захист інформацій в інформаційно-телекомунікаційних системах» (ІТС), «Про електронні документи та електронний документообіг», інструкція «Порядок підключення до глобальних мереж передачі даних» та багато інших. Нормативно-правові документи визначають не лише права, але й відповідальність користувачів за порушення у сфері інформаційної безпеки.

Інформаційна безпека для особистості має дві складові: **інформаційно-технічну та інформаційно-психологічну безпеку.**

Інформаційно-технічна складова передбачає забезпечення цілісності, конфіденційності та доступності до інформації. Цілісність передбачає захист інформації від модифікації, руйнування, знищення неавторизованими користувачами або процесом. Конфіденційна інформація — це інформація про фізичну або юридичну особу, доступ та поширення якої можливі лише за згодою її власника. Доступність інформації — це властивість, яка полягає в тому, що користувач, який володіє відповідними повноваженнями, може використовувати інформацію за встановленими правилами. **Інформаційно-психологічна безпека** спрямована на захист людини від брудної, недостовірної, шкідливої інформації, яка може негативно впливати на нервовий та психологічний стан людини.

Важливою складовою інформаційної безпеки є комп'ютерна безпека, яка передбачає захист даних від крадіжки або втрати, а також забезпечення надійної роботи комп'ютерної системи. Існують різні джерела загроз комп'ютерної безпеки: шкідливі програми різного типу, хакерські атаки, шпигунські програми, піратське програмне забезпечення, відвідування вредоносних сайтів тощо.

Шкідливі програми — це спеціально розроблені програми для пошкодження та знищення файлів даних і програмного забезпечення, викрадення особистих даних і коштів користувача. Ці програми можуть потрапляти в комп'ютер різними шляхами, наприклад:

- під виглядом ігрових та інших програм, скачаних з Інтернету;
- під час перегляду веб-сторінок;
- електронною поштою у додатках до листа;
- у процесі копіювання файлів з інших носіїв, які до цього використовувалися на заражених комп'ютерах.

Серед шкідливих програм розрізняють:

- комп'ютерні віруси;
- шпигунські програми.

Комп'ютерні віруси — це невеличкі програми, що потрапляють у комп'ютер з іншого носія даних або комп'ютерною мережею і виконують шкідливі дії, запрограмованими їх розробниками.

Як правило, спочатку їх дії є непомітними, а пізніше раптом порушуються файли або нормальна робота комп'ютера. Інколи вони починають діяти після певної дати, наприклад, після 21 травня. Віруси можуть знищувати файли і папки, повністю знищувати інформацію на диску, блокувати роботу комп'ютера, ви-

давати на екран незрозумілі повідомлення тощо. Деякі віруси можуть пошкодити й апаратні засоби. Найчастіше вони розміщуються у файлах, що виконуються (exe, com, sys, dll)й активізуються під час завантаження операційної системи. Такі віруси називають завантажувальними. Часто вони потрапляють і розповсюджуються комп'ютерною мережею, а також розміщуються у файлах документів, у яких застосовуються макроси. Тому віруси руйнують не лише додатки, але й файли даних. Для захисту комп'ютера від вірусів розроблена значна кількість антивірусних програм.

Шпигунські програми потрапляють у комп'ютер, зазвичай, мережею. Вони не самовідтворюються і тому їх не можна назвати вірусами. Головне їх призначення — слідкувати за діями, що виконуються на комп'ютері, і, наприклад, після підключення до Інтернету відправляти на сайт хакерів встановлені коди, паролі входження у платіжні системи, інтернет-магазин та інші дані. Вони можуть викрасти дані банківської картки, а потім і кошти. За рахунок користувача шпигунські програми можуть розсилати тисячі рекламних листів. Крім того, цей клас програм також може порушувати дані й нормальну роботу комп'ютера. До таких програм відносяться **троянські коні** (трояни) і **хробаки**.

Особливим видом комп'ютерних загроз є **хакерські атаки**, однією з яких є **фітинг**. Ця атака полягає у спонуканні користувача ввести свої автентифікаційні дані (логін, пароль, банківські дані та інші). Потім комп'ютерні шахраї за допомогою цих даних можуть нанести значну матеріальну, фінансову та іншу шкоду.

Існують два основних види захисту інформації в комп'ютерних системах: технічні й криптографічні.

Технічний захист інформації спрямований на забезпечення за допомогою технічних і програмних засобів унеможливлення вітоку, знищення та блокування інформації, порушення цілісності та режиму доступу до неї.

Криптографічний захист інформації реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Для забезпечення надійної роботи комп'ютера і збереження даних слід дотримуватися таких правил:

- не користуватися піратськими копіями програмного забезпечення;
- регулярно оновлювати ОС та інше програмне забезпечення;
- не запускати на виконання невідомі Вам програми;
- регулярно створювати резервні копії файлів даних на зовнішніх запам'ятовуючих пристроях;
- запускати на виконання лише ті програми і відкривати ті файли, що були перевірені на наявність вірусів;
- на комп'ютері потрібно мати програму захисту від вірусів, що функціонує безперервно і постійно оновлює свою базу знань;
- у процесі користування Інтернетом не переходити на невідомі посилання;
- користуватися паролями, не залишати комп'ютер без нагляду.

Друга проблема, що виникає під час вивчення комп'ютерної безпеки, полягає у виборі антивірусної програми й методики її вивчення учнями. Аналіз існуючих антивірусних програм дозволяє зробити висновок, що на сьогодні найбільш доступною для учнів є програма avast!. Вона забезпечує високий ступінь захисту комп'ютера від вірусів та інших шкідливих програм. Програма функціонує на платформах Windows, Linux, Palm, Android. Існують платні версії програми і безкоштовна версія Free. Далі розглядаються основні відомості про безкоштовну програму avast! Free.

Після установки avast! Free вона працює 30 діб, потім потрібна безкоштовна реєстрація. Програма функціонує у фоновому режимі й режимі сканера. У фоновому режимі перевіряються файли комп'ютера, електронна пошта, локальна мережа і Інтернет. Після встановлення програми вона функціонує у фоновому режимі і не потрібно виконувати ніяких додаткових дій, вона самостійно захищає комп'ютер від усіх відомих форм шкідливих програм. Резидентний сканер перевіряє ПК у режимі реального часу. Можна сканувати окремі носії, папки, виконувати експрес і повну перевірку системи. Автоматично здійснюється оновлення як самої програми, так і вірусної бази. Файли, що викликають підозру, переміщуються в карантин, з якого запустити їх неможливо. Програму avast! можна настроювати на власні потреби.

Кнопка програми avast! знаходиться, зазвичай, на панелі завдань, тому для її запуску достатньо клацнути цю кнопку. Після запуску програми avast! відкриється її головна сторінка, у якій відображується стан програми. Один із можливих варіантів вмісту сторінки у відкритому розділі **Статус** наведено на рис. 1.

Головна сторінка складається з чотирьох основних частин. Ліворуч (темний колір) — це розділи програми. Ліворуч зверху розташовано табло, у якому відображуються результати роботи програми. У даному випадку в табло висвітився рядок з повідомленням зеленого кольору — **Усе гаразд**. Це означає, що усі модулі програми оновлені й функціонують правильно. У цьому табло може бути й повідомлення червоним кольором — **Увага**. Це означає, що антивірусна программа застаріла. Повідомлення **Ви не захищені** свідчить, що комп'ютер взагалі не захищений. Якщо висвітиться друге або третєз наведених повідомлень, то у вікні з'явиться ще й кнопка **Виправити все**. Можна спробувати виправити стан програми, натиснувши цю кнопку. Нижче на головній сторінці розташована панель швидкого доступу з чотирма кнопками найчастіше використовуємих функцій програми (Експрес-сканування та інші). Користувач може самостійно замінити будь-яку з цих кнопок іншою. Нижче панелі швидкого доступу — це реклама.

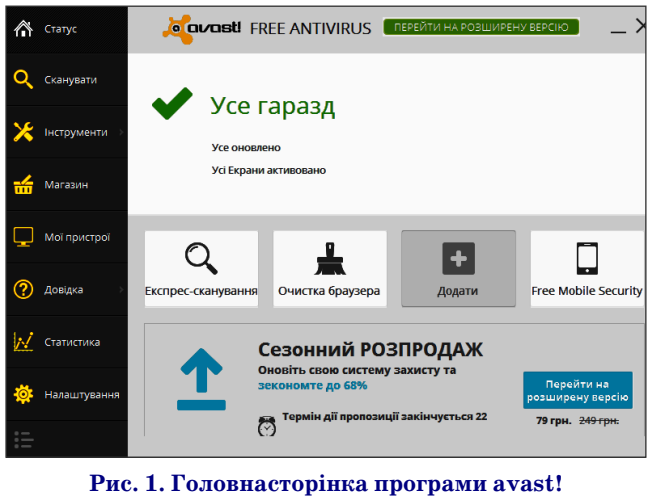

Рис. 1. Головнасторінка програми avast!

Виділимо розділ **Сканувати** і натиснемо у табло галочку. Відриються 5 видів сканування, наведених на рис. 2.

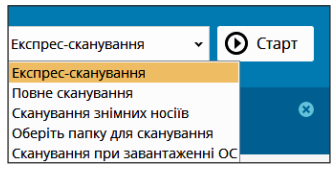

Рис. 2. Види сканування

Вид **Експрес-сканування** — це швидке сканування системного диска. За замовчуванням сканується оперативна пам'ять і системні файли (файли з розширенням exe, com, bat та інші). Під час виконання **Повного сканування** перевіряються усі файли на всіх дисках. Вид **Сканування з'ємних носіїв** забезпечує сканування flash-накопичувачів і CD/DVD дисків. Для сканування окремих папок або файлів використовується вид **Оберіть папку для сканування**. Вид **Сканування при завантаженні ОС** забезпечує перевірку комп'ютерана етапі завантаження ОС. Для запуску одного з наведених видів сканування необхідно виділити його і натиснути кнопку **Старт**.

Перелік наведених на панелі швидкого доступу видів сканування можна змінити. Для цього слід натиснути кнопку **Додати** (див. рис. 1). У результаті відкриється повний список видів сканування, наведений на рис. 3.

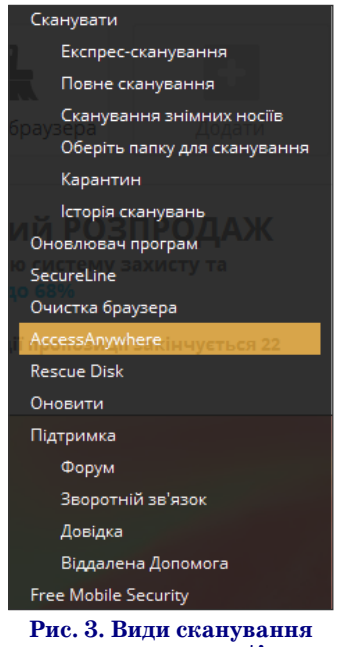

Рис. 3. Види сканування програми avast!

Якщо, наприклад, клацнути рядок **Повне сканування**, то кнопка цього виду сканування з'явиться на головній сторінці замість кнопки **Додати**. Потім кнопку **Додати** можна відновити. Для цього на відповідній кнопці натискують праву кнопку миші й у меню, що відкриється, виконується команда **Видалити ярлик**.

Якщо на комп'ютері встановлена програма avast!, то сканувати окремі папки або файли можна також за допомогою програми **Провідник**. Для цього у вікні програми **Провідник** слід відкрити контекстне меню файлу (папки) і виконати в ньому команду **Сканувати<ім'я файлу>**.

Експрес-сканування виконується декілька хвилин. Хід сканування відображується на екрані. Після завершення сканування на екрані відображуються його результати, один із можливих варіантів якого наведено на рис. 4.

Як видно з рисунка, загроз на комп'ютері не виявлено. Можна викликати на екран більш детальні результати сканування, у тому числі й результати попередніх сканувань. Для цього слід натиснути кнопку **Історія сканувань**, а потім виділити рядок сканування, виконаного 25.09.2014. На рис. 5 наведено приклад можливого результату сканування.

Рис. 4. Варіант результату експрес-сканування

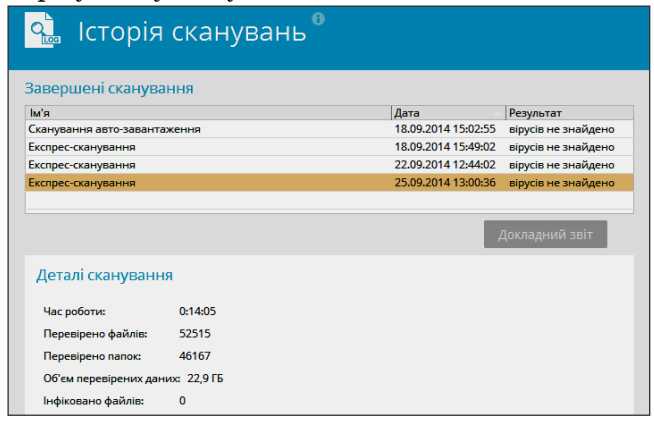

Рис. 5. Приклад результату експерс-сканування, виконаного 25.09.2014

У вікні наведена кількість перевірених папок, обсяг перевірених даних та інші відомості. Можна також переглянути статистичні дані про результати сканування. Для цього слід закрити вікно **Історія сканувань** і натиснути кнопку миші на розділі **Статистика**. На рис. 6 наведені статистичні результати сканування на вкладці **Ваша статистика** у розділі **Стан компонента**.

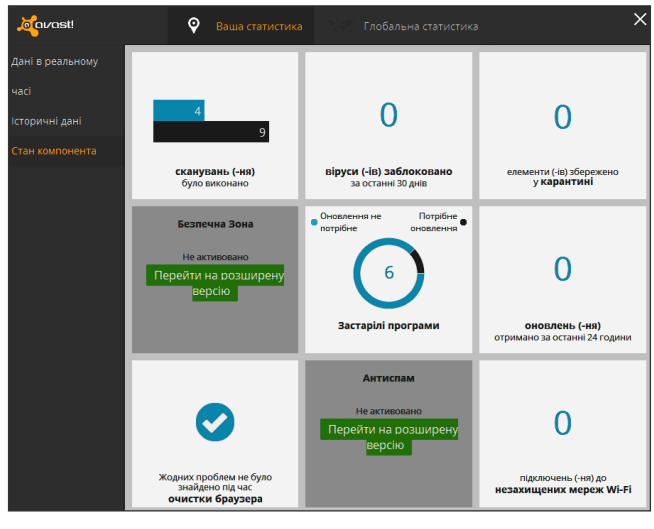

Рис. 6. Статистичні дані сканування

Повне сканування виконуватися 1–2 години. Варіант результатів повного сканування наведено на рис. 7.

З рисунка видно, що виявлено загрозу. Для перегляду загрози слід натиснути на кнопку **Показати результати**. У результаті отримаємо дані про місце знаходження і назви пошкоджених файлів. Приклад таких даних наведено на рис. 8.

У цьому вікні наведені імена і місце розташування інфікованих файлів. Якщо натиснути галочку у рядку **Виправити автоматично**, відкриється меню з переліком можливих дій, які можна виконувати над інфікованими файлами (рис. 9).

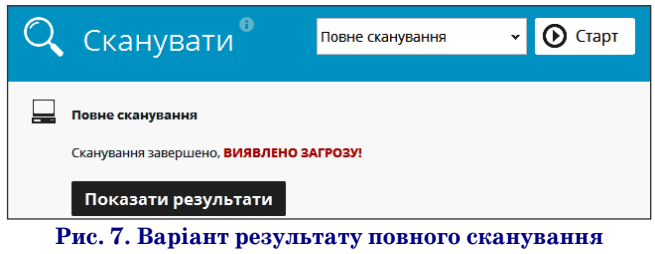

Рис. 7. Варіант результату повного сканування

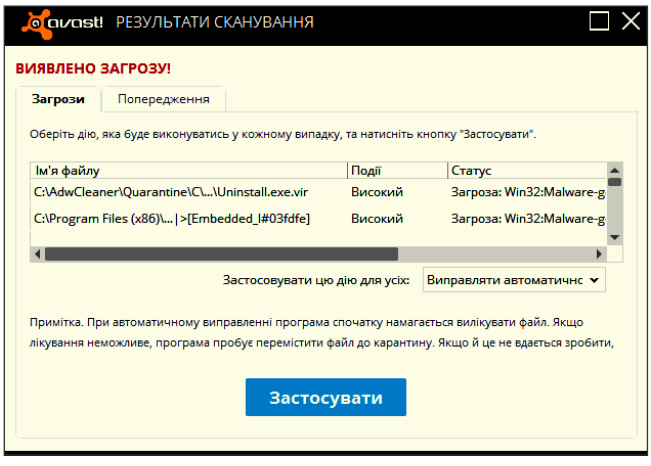

Рис. 8. Вікно з назвами пошкоджених програм

З рисунку видно, що інфіковані файли можна виправити автоматично, перемістити у карантин, лікувати, видалити і нічого не робити. Після вибору потрібної дії необхідно натиснути кнопку **Застосувати**. Слід однак враховувати, що лікування інфікованих файлів не завжди дає позитивний результат. У такому випадку такі файли доцільно перемістити у корзину або видалити.

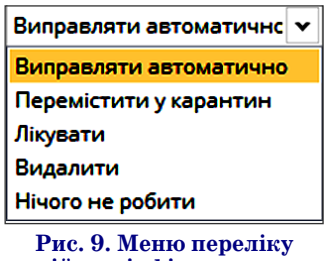

Рис. 9. Меню переліку дій над інфікованими файлами

Для закріплення знань і навичок доцільно запропонувати учням самостійно виконати такі завдання.

1. Розмістити на панелі швидкого доступу програми avast! кнопку **Довідка** (клацнути праву кнопку миші одну із кнопок панелі → **Змінити ярлик** → **Довідка**). Відкрити меню кнопки **Довідка** (клацніть цю кнопку). Ознайомтеся з вмістом основних пунктів меню: **Вітання**, **Користувацький інтерфейс** та інші.

2. Розмістити на панелі швидкого доступу програми avast! дві кнопки **Додати**, одну кнопку **Експрес-сканування** і одну кнопку **Повне сканування** (контекстне меню кнопки → **Видалити ярлик** → назва кнопки).

3. Виконати експрес-сканування комп'ютера. Призупиніть на деякий час сканування (для цього натисніть кнопку ⏸. Подивіться, який файл обробляється у даний момент. Продовжити сканування, для чого натисніть кнопку ▣. Зупиніть експрес-сканування, для чого натисніть кнопку ▣.

4. Переглянути, які файли знаходяться в карантині (**Сканувати** → **Карантин**).

5. Перевірити наявність антивірусних програм у магазині (відкрийте розділ **Магазин**). Відкрийте таблицю порівнянь антивірусних програм і проаналізуйте наведені у таблиці дані (клацніть рядок **Порівняння антивірусних програм**).

6. Виконати експрес-сканування власної флешки. Відкрийте вікно **Історія сканувань** і проаналізуйте деталі сканування флешки.

7. Виконати експрес-сканування однієї з папок робочого столу. Для цього відкрийте розділ **Сканувати**. Виберіть вид **Оберіть папку для сканування** і запустіть його. У вікні **Оберіть області**, варіант змісту якого наведено на рис. 10, виберіть одну з папок, наприклад csf, (для цього увімкніть прапорець біля назви папки) і натисніть кнопку **ОК**.

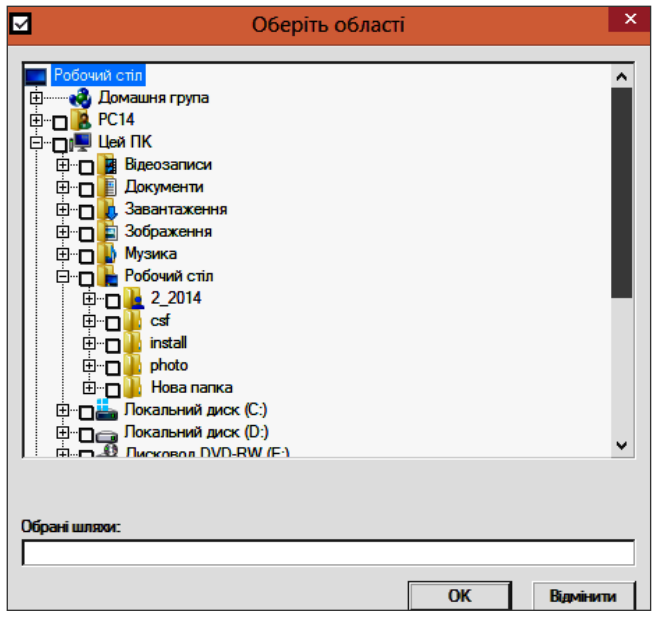

Рис. 10

Відкрити вікно **Історія сканувань** і переконатися, що папка просканована.

Отже, вивчення основ інформаційної безпеки у сьомому класі доцільно починати із загальних положень про інформаційну безпеку держави й особистості. Потрібно навести документи, що регламентують інформаційну безпеку, права і відповідальність людини у сфері інформаційної безпеки. Особливу увагу слід приділити правилам, яких слід дотримуватися під час роботи на комп'ютері. Як приклад антивірусної програми необхідно розглядати програму avast! Free.

★ ★ ★

Руденко В. Д. Содержание и методика изучения основ информационной безопасности в 7 классе

Аннотация. Обосновано содержание и методика изучения основ информационной безопасности в седьмом классе, приведены правила, каких следует придерживаться для надежной работы компьютера и сохранения данных, описаны основные возможности программы avast!, предложена методика работы в среде avast! Free.

Ключевые слова: информационная безопасность, компьютерная безопасность, компьютерные вирусы, шкодливые программы, антивирусы, avast!.

★ ★ ★

Rudenko Victor. Study of fundamentals of information security in 7th grade. Content and methodology

Resume. Grounded content and methodology of learning the basics of information security in the 7th grade, provided rules to be followed to secure the computer and data, described the main features of avast! antivirus software, proposed the methodology of usage of avast! Free software.

Keywords: information security, computer security, computer viruses, malware, antivirus, avast!.

Список використаних джерел

1. Навчальна програма. Інформатика. 5–9 класи загальноосвітніх навчальних закладів з поглибленим вивченням предметів природничо-математичного циклу; За ред. академіків НАПН України А. М. Гуржія і В. Ю. Бикова //Комп'ютер у школі та сім'ї. — 2012. — №6. — С. 3–14.
2. *Завадський І. О. та інші.* Інформатика: 9 кл.: Підруч. для загальноосвіт. навч. закл./ Ш. О. Завадский, І. В. Стеценко, О. М. Левченко. — К.: Видавнича група BHV, 2009. — 320 с. : іл.
3. *Руденко В. Д. та ін.* Базовий курс інформатики / В. Д. Руденко, О. М. Макарчук, М. О. Патланжоглу; За заг. ред.. В. Ю. Бикова: [Навч. посіб.]. — К.: Вид. група BHV. Кн. 1: Основи інформатики. — 2005. — 320 с.:іл.