

17.02.2022

Урок 26-27

Тема уроку: Забезпечення захисту інформації на комп'ютерному обладнанні та у локальних мережах

Мета уроку: ознайомлення з основними видами загроз КО у ЛМ.

Матеріали уроку:

Види загроз та рівні небезпеки інформаційних систем

Найбільш широко загрози інформаційним ресурсам можна розглядати як потенційно можливі випадки природного, технічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, яка зберігається в ній. Виникнення загрози характеризується уразливістю.

Види загроз інформаційній системі

Загроза розкриття інформаційних ресурсів полягає у тому, що дані, інформація стають відомими тим, кому не слід цього знати.

Загроза порушення цілісності інформаційних ресурсів – вплив (модифікація, видалення, зниження) даних, які зберігаються в інформаційній системі суб'єкта управління.

Класифікація загроз

- Апаратні засоби (блоки, вузли і готові вироби), якими оснащаються комп'ютери і мережі;
- Носії програмного забезпечення та інформації;
- Тверді копії з роздрукованою інформацією.

Джерелами помилок у програмному забезпеченні (ПЗ) можуть бути:

- Логічні помилки розробників програмного забезпечення;
- Непередбачувані ситуації, які проявляються при модернізації, заміні чи додаванні нових апаратних засобів, встановлених нових додатків, виходи на нові режими роботи ПЗ, появі раніше не зафікованих нештатних ситуацій;
- Віруси, якими інфіковані програми;

- Спеціальні програмні компоненти, які передбачені розробниками ПЗ для різного роду цілей.

Захист інформації в інформаційних системах

Сукупність методів і засобів захисту інформації включає програмні й апаратні засоби, захисні перетворення та організаційні заходи.

Апаратний, або схемний, захист полягає в тому, що в приладах ЕОМ та інших технічних засобах обробки інформації передбачається наявність спеціальних схем, що забезпечують захист і контроль інформації.

Програмні методи захисту – це сукупність алгоритмів і програм, які забезпечують розмежування доступу та виключення несанкціонованого використання інформації.

Захисні перетворення полягають в тому, що інформація, яка зберігається в системі та передається каналами зв'язку, подається в деякому коді, що включає її безпосереднє використання.

Організаційні заходи із захисту інформаціїмістять сукупність дій з підбору та перевірки персоналу, який бере участь у підготовці й експлуатації програм та інформації.

Вірус – програма, яка записується, перезаписується самостійно.

Антивірусні програми. Ці програми призначені для захисту від спеціально створених програм пошкодження інформації – вірусів.

Розрізняються за такими ознаками.

Середовище перебування. Віруси поділяються на:

- **Файлові**-ті, що додаються до файлів з розширенням exe, com;
- **Завантажувальні**-ті, що додаються до boot-сектора;
- **Мережні**-ті, що поширяються на комп’ютерній мережі;
- **Макровіруси**-ті, що заражають файли MicrosoftOffice. Вони пошкоджують копію шаблону Normal.dot, який завантажується в оперативну пам’ять комп’ютера під час роботи і наслідок чого всі файли, з якими проводиться робота, стають ураженими.

Способи зараження комп'ютера. Існують віруси:

- **Резидентні** – ті, що вміщуються в оперативну пам'ять і додаються до всіх об'єктів (файлів, дисків), до яких звертається ОС;
- **Нерезидентні** – ті, що додаються до оперативної пам'яті і є активними лише в короткий час.

Функціональні можливості. Такі групи вірусів:

- **Нешкідливі** - ті, що впливають на роботу комп'ютера (наприклад, збільшують розмір файлу);
- **Безпечні** - ті, що заважають роботі, але не пошкоджують інформацію (наприклад, дають якість повідомлення, перезавантажують комп'ютер тощо);
- **Небезпечні** - ті, що пошкоджують інформацію файлів, зумовлюючи «зависання» комп'ютера;
- **Дуже небезпечні** - ті, що зумовлюють утрату програм, знищення інформації із системних областей, форматування жорсткого диска.

Особливості алгоритму. Віруси поділяють на такі групи:

- **Віруси-супутники** – віруси, які не змінюють файли, але створюють одноіменні файли з розширенням .com, що завантажуються першими;
- **Віруси-черв'яки** – віруси, що поширюються автоматично в комп'ютерній мережі за знайденою адресою в адресній книзі;
- **Віруси-паразити** – віруси, які розпізнаються за зміненим змістом дискових секторів і файлів;
- **Stealth-віруси** – ті, що фальсифікують інформацію, яка читається з диска. Вірус перехоплює вектор переривання int 13hi видає активній програмі хибну інформацію, яка показує, що на диску все гаразд. Цей засіб використовується як у файлових, так і в завантажувальних вірусах;
- **Віруси-мутанти** – віруси, що мають зашифрований програмний код;
- **Ретровіруси** – звичайні файлові віруси, які намагаються заразити антивірусні програми, щоб знищити їх або зробити недієздатними.

Антивірусні програми, що дають змогу виявити вірус, від коректувати або вилучити пошкоджені файли, поділяють на детектори, фаги (лікарі), ревізори, сторожі, вакцини.

Детектори (сканери) перевіряють оперативну або зовнішню пам'ять на наявність вірусу за допомогою розрахованої контрольної суми або сигнатури (частина коду, що повторюється) і складають список ушкоджених програм. Детектором є, наприклад, програма MSAntiVirus.

Фаги (поліграфи) – виявляють та знешкоджують вірус (фаг) або кілька вірусів. Сучасні версії поліфагів, як правило можуть проводити евристичний аналіз файла, досліджуючи його на наявність коду, характерного для вірусу. Фагами є програми Aidtest, DrWeb.

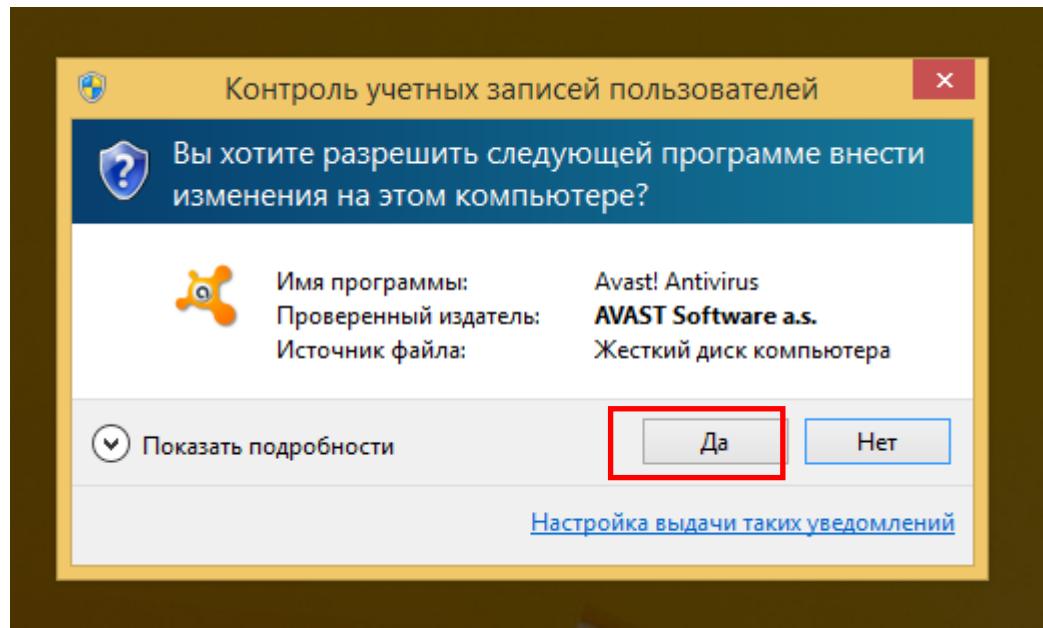
Ревізори – програми, що контролюють можливі засоби зараження комп'ютера, тобто вони можуть виявити вірус, невідомій програмі. Ревізором є програма Adinf.

Сторожі – резидентні програми, які постійно зберігаються у пам'яті й у визначений користувачем час перевіряють оперативну пам'ять комп'ютера. Сторожем є програма AVP, що може виявити понад 30 тис. вірусів.

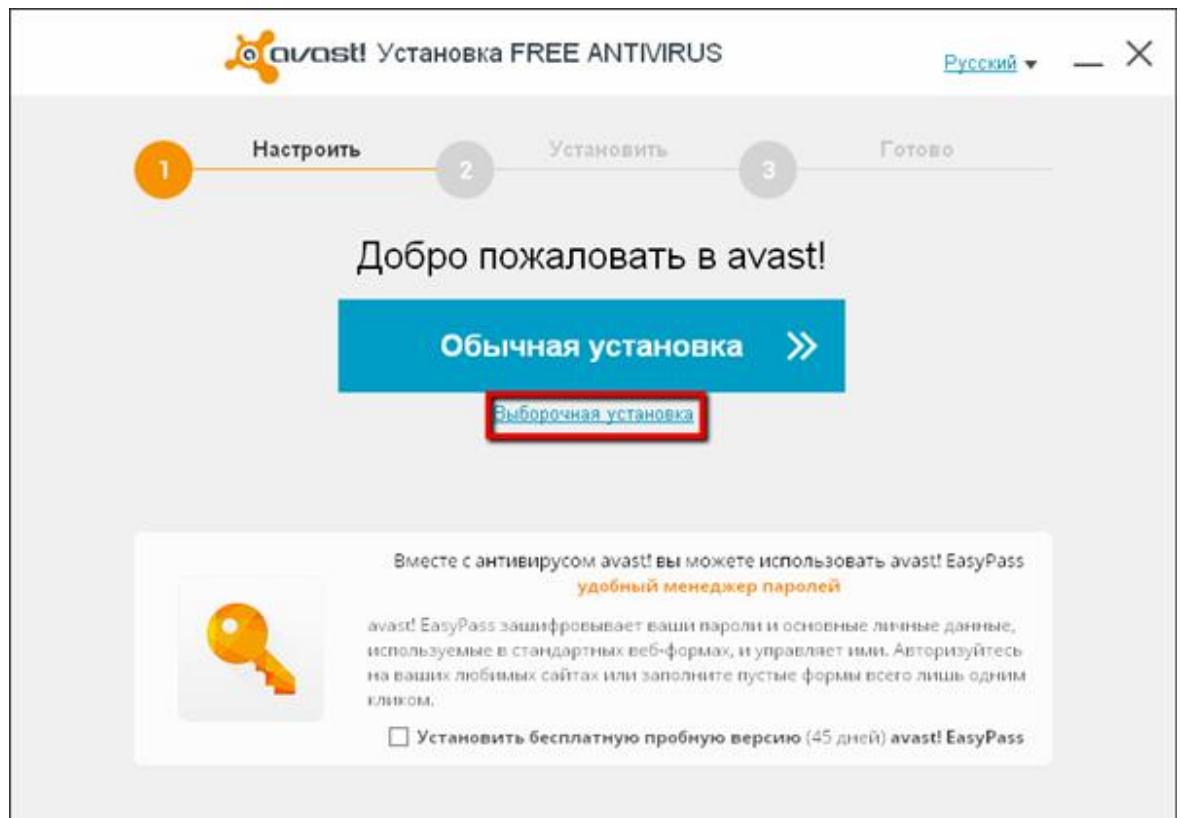
Вакцини – програми, які використовуються для оброблення файлів та завантажувальних секторів з метою передчасного виявлення вірусів.

Порядок встановлення та налагодження антивірусного програмного забезпечення

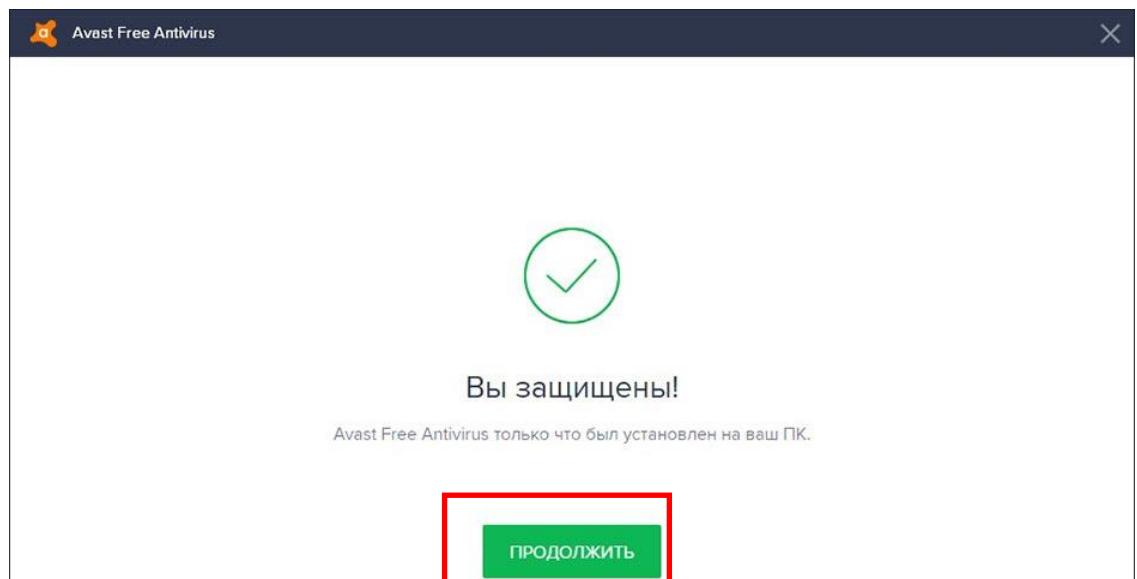
Завантажити антивірусну програму з мережі інтернет або з флеш – носія. Двічі класнути по вже завантаженій програмі, з'явиться вікно дозволу запуску програми, натиснути «Так».



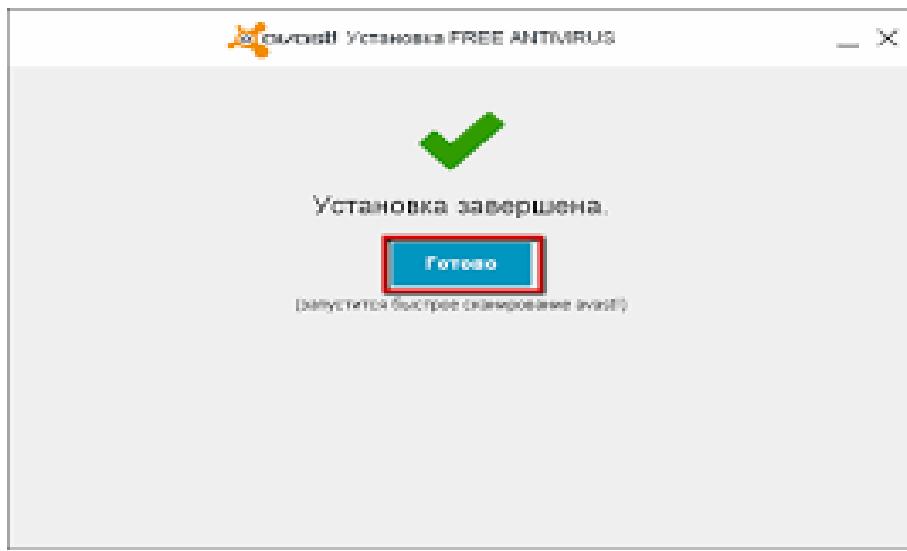
У вікні установки антивіруса вибрати пункт «Звичайне завантаження».



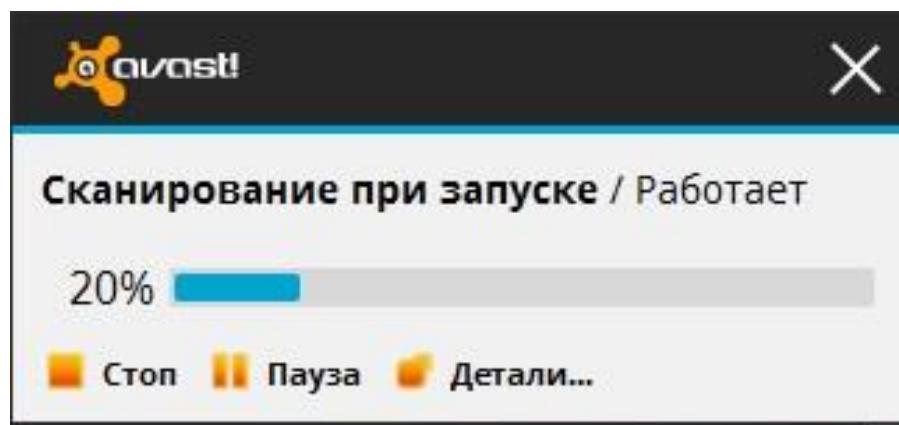
На наступному кроці натиснути клавішу «Продовжити»,



зачекати закінчення завантаження програми, з'явиться вікно у якому натиснути кнопку «Готово»



сканування програм розпочнеться автоматично.



Вибір типу сканування

На додаток до екранів антивіруса програма Avast Antivirus включає наступні види сканування.

- **Інтелектуальне сканування** : всебічне сканування, яке виявляє шкідливе ПО, програми, що вимагають оновлення, додаткові компоненти браузера з низькою репутацією, мережеві загрози, проблеми з продуктивністю, а також ненадійні, що повторюються і скомпрометовані паролі.

• **Повне сканування** : стандартний вид глибокого сканування системи з перевіркою дисків сховища і пам'яті на наявність шкідливого ПЗ.

• **Експрес-сканування** : сканування основного диска вашого ПК (на якому зберігаються системні файли) і автоматично запускаються програми, а також перевірка наявності всіх відомих типів руткітів. Щоб прискорити сканування, аналізуються тільки потенційно вразливі типи файлів.

• **Сканування USB / DVD** : сканування всіх знімних пристройів зберігання, підключених до ПК. Наприклад, зовнішніх жорстких дисків, флешнакопичувачів USB, дисків CD і DVD.

• **Сканування папок** : перевірка папок, обраних перед запуском сканування.

• **Сканування при завантаженні OS** : сканування комп'ютера при наступному перезапуску системи до запуску шкідливого ПЗ. Сканування під час завантаження підвищує шанси виявити і видалити шкідливі програми до того, як воно отримає можливість діяти.

Контрольні питання:

Як відбувається Запуск сканування?

Які налаштування потрібно використовувати?

Дати відповіді на запитання надсилати на адресу
olia.dubina2017@gmail.com

У темі листа вказати номер групи, прізвище та ім'я.