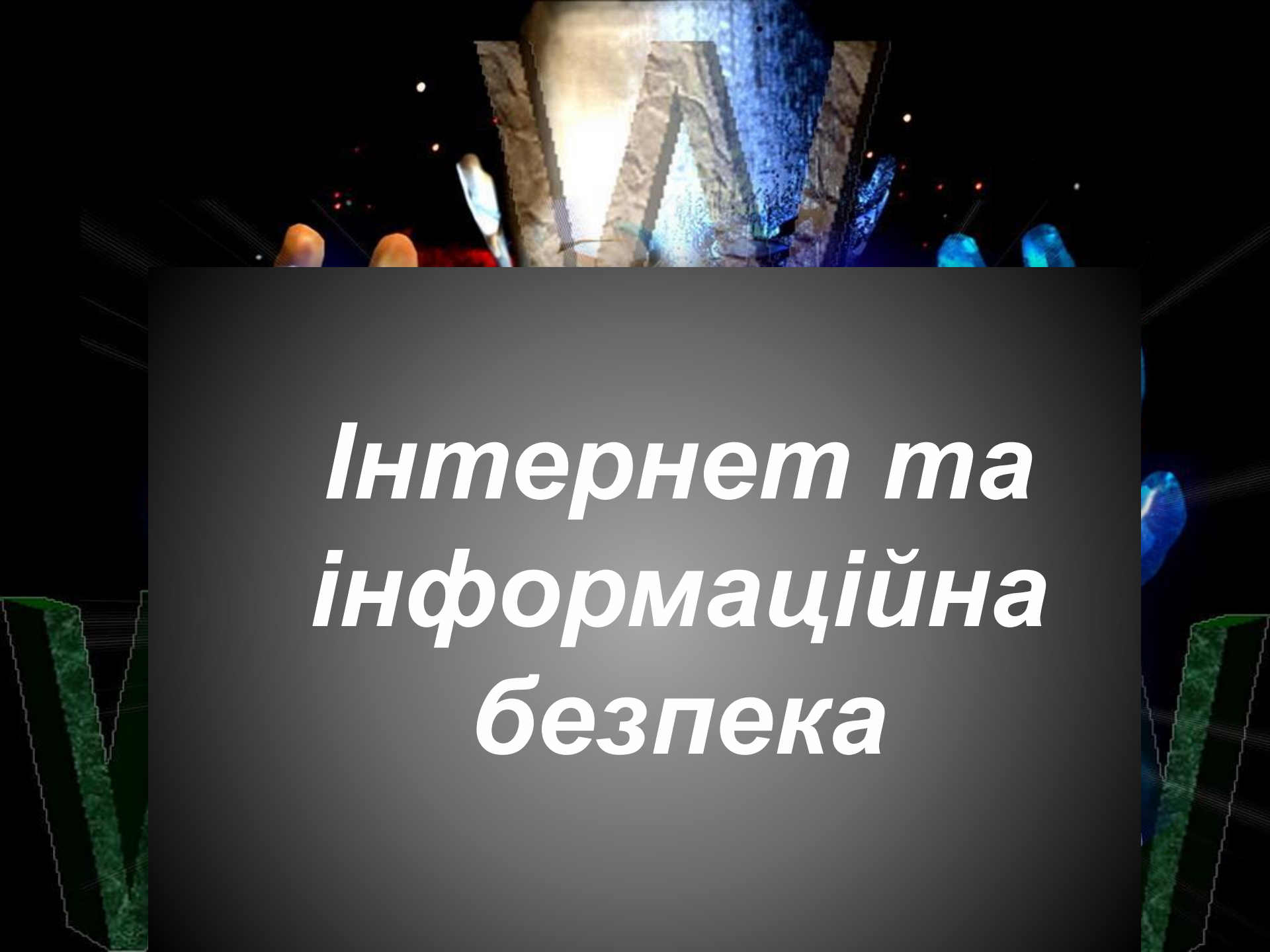


Інтернет та інформаційна безпека

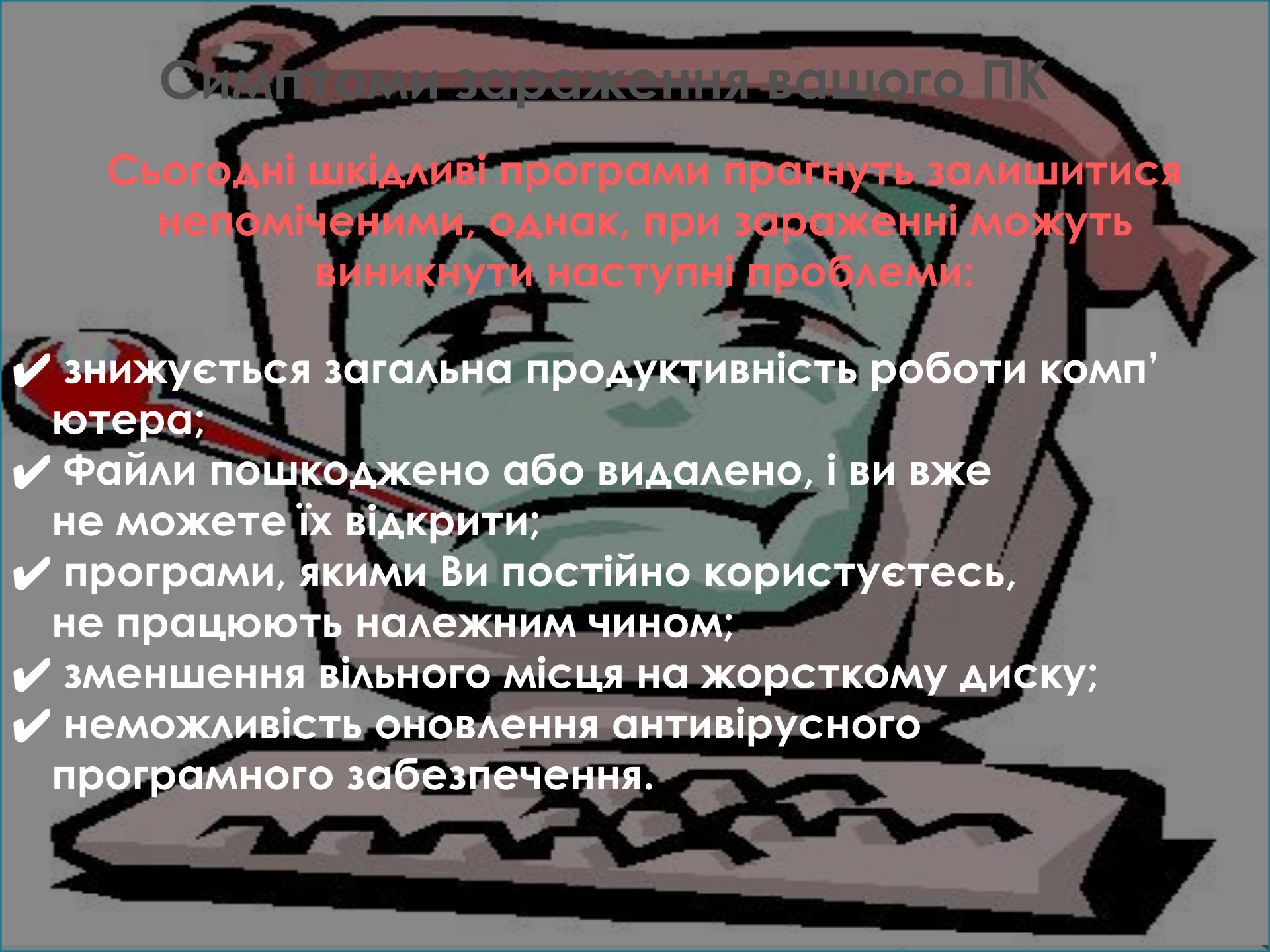
Загрози що походять з інтернету

Віруси, трояни, черв'яки та інші види шкідливого коду:

Віруси — це шкідливий програмний код, який заражає програми.

Сьогодні віруси в класичному вигляді зустрічаються досить рідко.

Поняття «**вірус**» вже давно переросло своє початкове значення і тепер часто вживається для позначення усіх шкідливих програм, здатних «розмножуватися» (поширюючись з комп'ютера на комп'ютер), заражаючи не тільки окремі локальні комп'ютерні мережі, а й спричиняючи глобальні епідемії в Інтернеті.



Симптоми зараження вашого ПК

Сьогодні шкідливі програми прагнуть залишитися непоміченими, однак, при зараженні можуть виникнути наступні проблеми:

- ✔ знижується загальна продуктивність роботи комп'ютера;
- ✔ Файли пошкоджено або видалено, і ви вже не можете їх відкрити;
- ✔ програми, якими Ви постійно користуєтесь, не працюють належним чином;
- ✔ зменшення вільного місця на жорсткому диску;
- ✔ неможливість оновлення антивірусного програмного забезпечення.

Результатом «роботи» вірусу може бути:

Відносно нешкідливі втручання в роботу комп'ютера — наприклад, злий жарт, коли екран гасне і показується повідомлення, що Ваш жорсткий диск пошкоджений;

завдання реальної шкоди — наприклад, коли змінюються або стираються важливі файли;

«кібер-злочин» — коли за допомогою троянських програм зловмисники отримують доступ до номерів Ваших кредитних карток, паролів доступу та іншої конфіденційної інформації.

Теперішні віруси — це класичні віруси, макровіруси, трояни, скрипт-віруси, поштові та мережеві черв'яки, боти і ботнет (botnet).

Бот — це програма, яка таємно, як правило — самостійно, встановлюється на Вашому ПК і виконує команди з так званого «командного центру». Сукупність керованих ботів називається «ботнетом».

- Виділення домену дає змогу швидше побачити дійсні веб-адреси на сайтах, які ви відвідуєте. Це допомагає уникнути переходу до обманних або фішингових веб-сайтів, які використовують недійсні веб-адреси, щоб заплутати користувачів. Під час відвідування справжнього домену його адреса виділяється в рядку адреси.

- Фільтр SmartScreen допомагає захистити комп’ютер від фішингових атак, шахрайства, а також від фальшивих і зловмисних веб-сайтів.

- Керування додатковими компонентами дозволяє вимкнути або ввімкнути додаткові компоненти браузера та видалити небажані елементи керування ActiveX.

- Захищене 128-бітне підключення (SSL) для використання безпечних веб-сайтів. Ця функція допомагає програмі Internet Explorer створювати шифроване підключення до веб-сайтів банків, онлайн-сховищ, медичних установ або інших організацій, які мають справу з конфіденційною інформацією споживачів.
- Фільтр перехресних міжсайтових сценаріїв (XSS) допомагає запобігати атакам фішингових і шахрайських веб-сайтів, які можуть намагатися викрасти особисту або фінансову інформацію.

У Windows також вбудовано засіб виправлення неполадок, який може автоматично усувати основні проблеми безпеки у браузері Internet Explorer.

Щоб відкрити засіб виправлення неполадок із безпекою Internet Explorer, натисніть кнопку Пуск і клацніть «Панель керування». У полі пошуку введіть виправлення неполадок і клацніть «Виправлення неполадок». Натисніть Переглянути все й виберіть пункт Безпека Internet Explorer.

Що теке спам?

Спам - це масові розсилки, реклама, та будь-яка інша інформація, яка надходить до вас всупереч вашій волі.

Спамом можуть бути в першу чергу електронні листи, пости та коментарі на блогах, форумах, інших сайтах, а також оффлайнова реклама.

Фішингове шахрайство

- **Фішинг** — це спосіб ошукання користувачів комп’ютерів з метою отримання приватної або фінансової інформації, наприклад, пароля банківського рахунку. Зазвичай фішингове шахрайство розпочинається з повідомлення електронної пошти, яке схоже на повідомлення від надійного джерела, однак насправді передає інформацію про користувача шахрайським веб-сайтам. Брандмауери не можуть визначити вміст електронного повідомлення, тому не захищають від таких атак. Для отримання

Засоби захисту від спаму чи наслідків його дії:

- Без потреби не публікуйте свою e-mail адресу будь-де
- без потреби не реєструйтесь на сайтах, форумах чи блогах - ви також передаєте їм свою інформацію, тим більше не треба реєструватись на підозрілих сайтах.

- Не відповідати на спам чи переходити за посиланнями, що містяться в ньому
- Користуватись останніми версіями браузерів, котрі самі визначають чи підозрюється сайт у фішингу (Firefox 3/Opera 9.5), а також останньою версією антивірусу
- Не тримати важливу інформацію в одному місці, завести хоча б кілька другорядних електронних скриньок

Статистичні методи фільтрації спаму

- Ці методи використовують статистичний аналіз змісту листа для прийняття рішення, чи є він спамом. Найбільшого успіху удалося досягти за допомогою алгоритмів, заснованих на теоремі Байеса. Для роботи цих методів потрібно «навчання» фільтрів, тобто потрібно використовувати розсортовані вручну листи для виявлення статистичних особливостей нормальних листів і спаму. Після навчання на досить великій вибірці, вдається розпізнати до 95-97 % спаму.