Нарощування шарів (рівнів групування) залежить від кількості вершин, та їх залежності одна від одної по місцезнаходженню.
Послідовне виконання алгоритму дає можливість рухаючись від вершин, по границям розмежування з'єднань, до середини найдовшого ребра, зібрати всі ребра в окремі пучки і в подальшому в єдиний джгут.

Список використаних джерел

1. Heer Jeffrey. A tour through the visualization zoo / Heer Jeffrey; Bostock Michael; Ogievetsky Vadim – Communications of the ACM, 2010. – С. 59-67.
2. Візуалізація графів [Електронний ресурс]: веб-ресурс science-community. – Режим доступу https://www.science-community.org/en/node/5582

УДК 004.07

Сімон К.А., здобувачка 3 курсу спеціальності 122 «Комп'ютерні науки»
Горяшин А.С., асистент кафедри інформаційних технологій

ЗАХИСТ ІНФОРМАЦІЇ ПІД ЧАС РОБОТИ В ІНТЕРНЕТІ

Донецький національний університет імені В. Стуса, м. Вінниця

Інформаційна загроза — це потенційна можливість певним чином порушити інформаційну безпеку.

Під інформаційною безпекою розуміють захищеність даних та інфраструктури, що її підтримує, від будь-яких випадкових або зловмисних дій, результатом яких може стати нанесення шкоди безпосередньо даним, їхнім власникам або інфраструктурі, що підтримує інформаційну безпеку [1].

Види загроз інформаційній безпеці:

- отримання доступу до секретних або конфіденційних даних;
- порушення або повне припинення роботи комп'ютерної інформаційної системи;
- отримання доступу до керування роботою комп'ютерної інформаційної системи;
- знищення або спотворення даних.

Дані можуть бути відкриті, до деяких даних має доступ тільки певна група людей, а деякі дані — особисті, до них доступ може мати тільки одна людина.

Існує досить багато загроз. Основні з них:

- Потрапляння в інформаційну систему шкідливого

програмного забезпечення: вірусів, троянських програм, мережевих хробаків, клавіатурних шпигунів, рекламних систем;

- Атаки хакерів;
- DdoS — атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні;
- Фішинг — вид шахрайства, метою якого є виманювання персональних даних у клієнтів онлайн-аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів тощо [2].

Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об'єднати у такі групи: моральноетичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Зокрема, сучасні технології розвиваються в напрямку сполучення програмних та апаратних засобів захисту.

Для виявлення, знищення та попередження «електронних інфекцій» можна використовувати загальні засоби захисту інформації (копіювання інформації, розмежовування доступу до неї) та профілактичні заходи, які зменшують імовірність зараження. Останніми роками з'являються апаратні пристрої антивірусного захисту, наприклад спеціальні антивіруси - плати, які вставляються у стандартні слоти розширення комп'ютера. Але найбільш поширеним методом залишається використання антивірусних програм — спеціальних програм, призначених для виявлення і знищення комп'ютерних вірусів.

Антивірусні програми поділяють на кілька видів:

- **Програми-детектори** здійснюють пошук сигнатур вірусів. Недоліком детекторів є те, що вони можуть знаходити тільки ті віруси, які відомі їхнім розробникам, а отже, вони швидко застарівають.
- **Програми-доктори («фаги»)** не тільки знаходять заражені вірусами файли, а й «лікують» їх (видаляють з файла тіло програ-ми-вірусу), повертаючи їх у початковий стан. Перед лікуванням файлів програма очищує оперативну пам'ять.
- **Програми-ревізори** запам'ятовують початковий стан програм, каталогів і системних областей, коли комп'ютер не заражений вірусом, а згодом, періодично або за бажанням користувача, порівнюють поточний стан системи з початковим. Як правило, перевірка здійснюється відразу після завантаження операційної системи — контролюються довжина файла, його контрольна сума, дата і час модифікації та інші параметри.
- **Програми-фільтри («сторожа», «монітори**») — резиденти програми, призначені для виявлення підозрілих дій при роботі комп'ютера. Після одержання відповідного повідомлення користувач може дозволити або відмінити виконання операції.
- **Програми-вакцини («іммунізатори»)** модифікують програми і диски таким чином, що це не відбивається на роботі програм,

але вірус, від якого проводиться вакцинація, вважає їх інфікованими. Це вкрай неефективний спосіб захисту.

Жодний з типів антивірусних програм не надає стовідсоткового захисту, тому слід додержувати загальних правил і користуватись останніми розробками антивірусних лабораторій [3].

Список використаних джерел

1. *https://mozok.click/2153-osnovi-nformacynoyi-bezpeki-zagrozi.html*
2. *https://miyklas.com.ua/p/informatica/10-klas/informatciini-tekhnologiyi-v-suspilstvi-322205/informatciina-bezpeka-navchannia-v-interneti-321523/re-0cf3c5d6-6a11-458b-b39d-889f102e9e71*
3. *К. Мандиа, К. Просис. Защита от вторжений. Расследование компьютерных преступлений.– М., 2005.*

УДК 004.05

Сімон К.А., здобувачка 3 курсу спеціальності 122 «Комп'ютерні науки»
Ніколюк П. К., професор кафедри інформаційних технологій

СУЧАСНЕ 3D МОДЕЛЮВАННЯ

Донецький національний університет імені В. Стуса, м. Вінниця

3D-моделі − невід'ємна складова якісних презентацій та технічної документації, а також – основа для створення прототипу виробу.

Тривимірна графіка або 3D-моделювання – комп'ютерна графіка, що поєднує в собі прийоми і інструменти, необхідні для створення об'ємних об'єктів в тривимірному просторі.

Об'ємний рендеринг – це створення двовимірного растрового зображення на основі побудованої 3D-моделі. Це максимально реалістичне зображення об'ємного графічного об'єкту. Області застосування 3D-моделювання:

Тривимірна графіка незамінна у презентації майбутнього виробу. Для того, щоб розпочати виробництво необхідно намалювати, а потім створити 3D-модель об'єкту. А вже на основі 3D-моделі, за допомогою технологій швидкого створення прототипів (3D-друк, фрезерування, лиття силіконових форм і т.д.), складається реалістичний прототип майбутнього виробу.

За допомогою тривимірної графіки досягається максимально реалістичне моделювання міської архітектури і ландшафтів з мінімальними витратами.