СПЕЦІАЛІЗОВАНІ ІНТЕРНЕТ-САЙТИ ДИТЯЧОЇ ЛІТЕРАТУРИ

- Весела абетка;
- Українська казка;
- Дитяча література;
- Левко;
- Країна міркувань;

ІНТЕРНЕТ-САЙТИ БІБЛІОТЕК ТА ЕЛЕКТРОННИХ БІБЛІОТЕК

- вебсайт Державної бібліотеки України для юнацтва (м. Київ);
- вебсайт Національної бібліотеки України імені В.І. Вернадського (м. Київ);
- вебсайт Державної наукової установи "Книжкова палата України імені Івана Федорова" (м. Київ);
- вебсайт "Бібліотеки в мережі Internet";
- вебсайт Рівненської обласної наукової бібліотеки http://libr.rv.ua/ua/

ОСВІТНЬО-ІНФОРМАЦІЙНІ РЕСУРСИ

- вебсайт Український мовно-інформаційний фонд НАН України "Словники України"
- вебсайт "Світ географії та туризму"
- ТОП-5 найцікавіших місць Рівненщини https://youtu.be/NiRbdu3qfKk
- Спадщина предків. Культурно-історичний портал https://spadok.org.ua/

ІНТЕРНЕТ-САЙТИ МУЗЕЇВ І КАРТИННИХ ГАЛЕРЕЙ УКРАЇНИ

- вебсайт Національного художнього музею України;
- вебсайт Музею театрального, музичного та кіномистецтва України;
- вебсайт Аптеки-музею Рівного https://www.youtube.com/watch?v=i_bqjFJfSzU
- вебсайт Рівненського обласного краєзнавчого музею http://museum.rv.gov.ua/

Існує досить багато інформаційних загроз. Основні з них:

• Потрапляння в інформаційну систему шкідливого програмного забезпечення: вірусів, троянських програм, мережевих хробаків, клавіатурних шпигунів, рекламних систем.
• Атаки хакерів.
• **BotNet** — це комп'ютерна мережа, що складається з деякої кількості хостів, із запущеними ботами — автономним програмним забезпеченням.
• **DdoS** — атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні (англ. DoS-attack (Distributed) Denial-of-service attack) — напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.
• **Фішинг** — вид шахрайства, метою якого є виманювання персональних даних у клієнтів онлайн-аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів тощо.
Для **смартфонів** характерні ті самі загрози, що і для стаціонарних комп’ютерів: віруси, троянські програми, мережеві хробаки, рекламні модулі тощо, орієнтовані на різні типи мобільних пристроїв.

Основні правила безпечної роботи в Інтернеті:

• Установлюйте та оновлюйте антивірусне програмне забезпечення як на стаціонарні, так і на мобільні комп’ютери. Бажано, щоб оновлення антивірусних баз здійснювалося регулярно та автоматично.
• Завжди встановлюйте оновлення операційної системи та іншого програмного забезпечення.
• Використовуйте надійні паролі. Не використовуйте на різних інтернет-ресурсах один і той самий пароль, змінюйте його регулярно.
• Приєднуйтеся тільки до перевірених Wi-Fi-мереж. Не відправляйте важливі дані (дані кредитних карток, онлайн-банкінгу тощо) через публічні та незахищені Wi-Fi-мережі.
• Установіть фільтр спливаючих вікон у браузері.
• Не відкривайте повідомлення електронної пошти від невідомих вам осіб і прикріплені до них файли, яких ви не очікуєте.
• Подумайте про можливі ризики для вас перед тим, як викласти щось у мережу Інтернет.

Рівненська загальноосвітня школа І-ІІІ ступенів №22 Рівненської міської ради

Корисні та безпечні сайти для дітей

Путівник для батьків

2020-2021 н.р.

Підготувала практичний психолог
Хвост Тетяна Володимирівна