Звіт  
По Практичному заняттю номер 3  
З основ інформаційної безпеки  
Студента Ларіонова Володимира  
  
Для виконання завдань 1-4 була написана одна загальна програма з інтерфейсом у терміналі. Працювати з проектом, який складається більш ніж з одного файлу, значно цікавіше ніж з відокремленими одна від одної програмами.  
  
Висновки:  
Складніші алгоритми хешування є більш безпечними та, зазвичай, криптографічно стійкішими. Проте вони також більш повільні і генерують хеш більшого розміру.

Пароль, який містить тільки невелику кількість символів, набагато легше підібрати. Якщо ж пароль містить тільки цифри (тільки букви), його криптографічна стійкість значно менша ніж у пароля такої ж довжини, але який містить відразу декілька типів символів (цифри, букви, спеціальні символи)  
За допомогою хешування можна досить легко перевірити аутентичність двох повідомлень, просто зіставивши їх шех-коди. Це дає змогу зберігати тільки хеш-код певних масивів інформації (наприклад, паролів), якщо важливо тільки переконатися у аутентичності збереженої та надісланої користувачем інформації.  
Сктурування коду робить навігацію по ньому більш зручнішою, а сам код – більш зрозумілим. Це спрощує як подальшу розробку программи саморуч, так і роботу у команді. Також виправляти помилки та боротися з багами у гарно структурованому коді значно зручніше та швидше.

Об’єднання проектів та минулих напрацювань прискорює написання нового коду та спрощує реалізацію завданнь.  
Github-репозиторій:

<https://github.com/LoUyyR12/Information-Security.git>