**Федеральное государственное бюджетное образовательное учреждение высшего образования "Белгородский государственный технологический университет им. В.Г. Шухова"**

Кафедра программного обеспечения вычислительной техники и автоматизированных систем.

**Лабораторная работа №1**

Работа с CNG.

Выполнил:

Студент группы КБ-211

Коренев Д.Н.

Принял:

Смакаев А.В.

Оглавление

[Задание 3](#_Toc177870085)

[Макеты страниц 3](#_Toc177870086)

[1. Главная страница 3](#_Toc177870087)

[2. Страница авторизации 4](#_Toc177870088)

[3. Контентная страница 5](#_Toc177870089)

[Код CSS 8](#_Toc177870090)

[Демонстрация внешнего вида разработанных страниц 15](#_Toc177870091)

[Вывод 16](#_Toc177870092)

*Цель работы:* ознакомится с криптографическим API операционных систем семейства Windows. Разработать консольное приложение, использующее CNG для генерации ключа и шифрования/дешифрования файлов. Исследовать лавинный эффект при разных режимах сцепления блоков.

Задание

1. Разработать консольное приложение, позволяющее генерировать ключи шифрования и шифровать/дешифровать файлы симметричным шифром AES с использованием криптографического API CNG.
2. Исследовать лавинный эффект при разных режимах сцепления блоков (ECB, CBC, CFB). В ходе исследования нужно
   1. произвести эксперимент по изменению каждого отдельного бита в открытом тексте;
   2. построить график зависимости количества измененных в шифротексте битов от позиции измененного бита в открытом тексте.