ЧУ ДО “Школа Программистов”
ИНН: 5029106464
Адрес: 141021, Московская область,
г. Мытищи, ул. Юбилейная, д. 13, корп.2
E-mail: info@informatics.ru
Телефон: 8 (498) 500-05-00

Курс “Компьютерные сети”

Информационная система для обучения основам криптографической защиты информации

Техническое задание
на 8 листах

Согласовано:

Преподаватель курса “Компьютерные сети”,
_____ Елисеев Р. А.
“__” _____ 2020 г.

Москва, 2020/2021 г.

СОДЕРЖАНИЕ

1. Общие сведения о проекте. **3**
1.1 Полное наименование системы и ее условные обозначения. 3
1.2 Сведения о заказчике и разработчике. 3
1.3 Основание для разработки ИС. 3
1.4 Плановые сроки начала и окончание работы ИС. 3
1.5 Источники финансирования для разработки ИС 3
1.6 Порядок оформления и предъявление заказчику результатов работоспособности системы. 3

2. Назначение и цели создания системы. **4**
2.1 Назначение системы. 4
2.2 Цели создания системы. 4

3. Характеристика объекта автоматизации. **5**
3.1 Краткие сведения об объекте автоматизации. 5
3.2 Сведения об условиях эксплуатации объекта. 5

4. Требования к системе. **6**
4.1 Требования к системе в целом. 6
4.1.1 Требования к функционированию и структуре информационной системы. 6
4.1.2 Требования к защите информации от несанкционированного доступа 7
4.2 Требования к задачам, выполняемым системой. 7

5. Состав и содержание работ по созданию системы. **8**

1. Общие сведения о проекте.

1.1 Полное наименование системы и ее условные обозначения.

Информационная система для обучения основам криптографической защиты информации.
Условное обозначение: ИС для обучения ОКЗИ.

1.2 Сведения о заказчике и разработчике.

Заказчик - Частное Учреждение Дополнительного Образования “Школа Программистов”.
Разработчик - Виноградов Владимир Андреевич, ученик 10И-2, Лицей Национального исследовательского университета «Высшая школа экономики».

1.3 Основание для разработки ИС.

Обновление курса “Компьютерные сети” в связи его модернизацией и внедрением нового программного обеспечения в образовательный процесс.

1.4 Плановые сроки начала и окончание работы ИС.

- Начало работ: начало зимы 2020
- Тестовое внедрение: середина осени 2021
- Окончание работ: конец осени 2021

1.5 Источники финансирования для разработки ИС

Собственные средства разработчика.

1.6 Порядок оформления и предъявление заказчику результатов работоспособности системы.

К результатам работы разработчика относятся:
- Оригинальное программное обеспечение
- Оригинальные структуры данных
- Проектная рабочая документация

Результаты заказчику передаются частями:
- Управление над репозиторием, в котором разрабатывался проект.
- Проектная рабочая документация

Разработчику предоставляется доступ к тестовому серверу, на котором можно проводить тестирование проекта.

2. Назначение и цели создания системы.

2.1 Назначение системы.

ИС для обучения ОКЗИ предназначена для автоматизации обучения по курсу “Компьютерные сети” и знакомства с основными механизмами криптографических алгоритмов.

2.2 Цели создания системы.

Целью создания системы является:

- Снижение нагрузки на преподавателя.
- Дать возможность ученикам поработать с системами шифрования.
- Визуализировать алгоритмы шифрования.
- Замена программных средств, потерявших актуальность.

3. Характеристика объекта автоматизации.

3.1 Краткие сведения об объекте автоматизации.

Объектом автоматизации является частичное наполнение курса “Компьютерные сети”, а именно занятия связанные с алгоритмами шифрования и их уязвимостями.

3.2 Сведения об условиях эксплуатации объекта.

- ИС для обучения ОКЗИ используется преподавателями и учениками курса “Компьютерные сети”.

Требования к функционированию объекта:

- Система должна эксплуатироваться в процессе занятия.
- При невозможности использования системы через глобальную сеть Интернет должна быть возможность использовать локальную копию информационной системы.

4. Требования к системе.

4.1 Требования к системе в целом.

4.1.1 Требования к функционированию и структуре информационной системы.

ИС для обучения ОКЗИ должна представлять собой систему, включающую в себя подсистемы:

- П/с Базы данных с заранее заготовленными алгоритмами шифрования.
- Подсистемы взаимодействия с выбранным шифром.
    - П/с шифрования.
    - П/с расшифрования.
    - П/с дешифрования.
- П/с загрузки пользовательских данных для шифрования.
- П/с выдачи подсказок для п/с дешифрования (для заранее заготовленного алгоритма шифрования).
- П/с конструктора с криптографическими примитивами.

Пояснение по функциям подсистем:

I. П/с Базы данных с заранее заготовленными алгоритмами шифрования
    - Для преподавателя и ученика должен быть выбор одного из заранее заготовленных алгоритмов шифрования.
    - Загружает в основную подсистему выбранный алгоритм шифрования

II. (Основные) Подсистемы взаимодействия с выбранным шифром
    - П/с шифрования должна предоставлять возможность зашифровать открытый текст при помощи выбранного алгоритма и ключа шифрования.
    - П/с расшифрования должна предоставлять возможность расшифровать шифротекст при помощи выбранного алгоритма и ключа шифрования.
    - П/с дешифрования должна предоставлять возможность дешифровать шифротекст с указанием алгоритма и без ключа шифрования.

III. П/с загрузки пользовательских данных для шифрования
    - Данная п/с взаимодействует с основной
    - Реализует возможность загрузить в систему открытый текст/зашифрованный текст для дальнейших процедур, указанных как подсистемы в пункте II.

IV. П/с выдачи подсказок для п/с дешифрования
    - Выдача подсказок для дешифрования
    - Необходимо для ускорения работы учеников

V. П/с конструктора с криптографическими примитивами.
    - Визуальный конструктор работы с криптографическими примитивами.
    - Возможность написать свой криптографический примитив.

4.1.2 Требования к защите информации от несанкционированного доступа

К ИС не предъявляется особых требований по защите информации. Все компоненты, разработанные заранее или разработанные в конструкторе являются информацией с открытым доступом.

4.2 Требования к задачам, выполняемым системой.

4.2.1 Перечень функций, подлежащих автоматизации.

I. *П/с Базы данных с заранее заготовленными алгоритмами шифрования*
Выполняет функцию хранилища заранее заготовленных алгоритмов шифрования и примеров к ним. При выборе алгоритма пользователем производится загрузка информации во внутренние структуры данных.

II. *(Основные) Подсистемы взаимодействия с выбранным шифром*
Основная подсистема-интерфейс для пользователя. Позволяет взаимодействовать с выбранными алгоритмами шифрования и производить заданные операции с шифрами. Необходимо предусмотреть три различных интерфейса для работы с операциями.

III. *П/с загрузки пользовательских данных для шифрования*
ИС подразумевает возможность загрузки пользовательских данных для шифрования и выгрузки зашифрованных данных. Также этот механизм используется в интерфейсе дешифрования для работы с заранее заготовленными данными.

IV. *П/с выдачи подсказок для п/с дешифрования*
Функция подсказок необходима для понимания работы некоторых частей алгоритма. Должен быть предусмотрен разный формат подсказок - от выявления одного байта ключа до подсказки по поводу строения ключа. Можно заметить, что подсказки так или иначе должны быть связаны с ключом.

V. *П/с конструктора с криптографическими примитивами.*
Данная подсистема представляет собой визуальный конструктор базирующийся на криптографических примитивах и базовых преобразованиях. Система предназначена для усиления понимания того, как влияют криптографические преобразования на открытый текст.

5. Состав и содержание работ по созданию системы.

Вести разработку предполагается при помощи плана, указанного в таблице 1.

Таблица 1.

Наименование стадий и этапов разработки проекта	Сроки выполнения работ	Результат работ
1. Создание эскизного проекта. 1.1 Разработка предварительных проектных решений.	02.12.2020-02.01.2021	Описание функций и подсистем, список используемых технологий и требуемых ресурсов.
2. Технический проект 2.1 Разработка подсистем проекта. 2.2 Разработка интерфейсов проекта.	02.01.2021 - 15.05.2021	Тестовый вариант системы, драфтовые варианты интерфейсов.
3. Технический проект 3.1 Доработка подсистем 3.2 Доработка интерфейсов	15.05.2021-01.10.2021	Доработка подсистем, итоговое тестирование подсистем, финальные варианты интерфейсов.
4. Итоговое тестирование проекта 4.4 Ввод проекта в действие	01.10.2021-29.10.2021	Итоговое тестирование проекта, сдача проекта заказчику.