ИНТЕРАКТИВНЫЙ УЧЕБНО-ИССЛЕДОВАТЕЛЬСКИЙ КОМПЛЕКС ДЛЯ ПОСТРОЕНИЯ И АНАЛИЗА АЛГОРИТМОВ ШИФРОВАНИЯ ИНФОРМАЦИИ

Рычкова А.А., Усманов Р.И.
Оренбургский государственный университета, г. Оренбург

В соответствии с требованиями ФГОС ВПО по направлению подготовки 090900.62 «Информационная безопасность» будущий бакалавр должен владеть «способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации». Для формирования данной компетенции в учебном плане ООП предусмотрено изучение общепрофессиональной дисциплины «Криптографические методы защиты информации, в ходе проведения которой будущие бакалавры получают знания об основных принципах построения криптографических алгоритмов, осваивают возможности их использования в информационных системах. Целью изучения дисциплины является формирование теоретических знаний основных криптографических алгоритмов и практических навыков их применения для защиты информации [1].

Для наглядного представления материала, визуализации криптографических преобразований, анализа построения и режимов работы алгоритмов шифрования на кафедре вычислительной техники и защиты информации авторами статьи разрабатывается интерактивный учебно-исследовательский комплекс, который возможно применять в учебном процессе наряду с существующими электронными образовательными ресурсами: электронными курсами лекций, учебными видеоматериалами, анимационными роликами, прикладными программами учебного назначения. Данные средства являются основой для применения наряду с традиционными формами обучения электронного обучения и дистанционных образовательных технологий [2, 3, 4].

Нами был проведен сравнительный анализ готовых программных средств визуализации алгоритмов шифрования (таблица 1).

Таблица 1 – Сравнительный анализ программных средств шифрования информации

Параметры	Программные средства шифрования информации			
	Эмулятор Enigma3S	Rijndael Cipher	Visual AES	CrypTool 2.1
Удобный интерфейс	-	+	+	-
Выбор методов	-	-	-	+
Трассировка алгоритма	+	+	+	+
«Слепое» шифрование	+	-	+	+
Математическая основа	+	-	-	+
Низкие затраты ресурсов	+	+	+	-

Проведенный сравнительный анализ позволил на основе выделенных параметров определить все достоинства и недостатки существующих аналогов, выявить необходимые требования для разработки авторского учебно-исследовательского комплекса построения и анализа шифрования информации.

Разрабатываемое программное средство предназначено для повышения уровня визуализации при проведении анализа и этапов реализации криптографических преобразований при изучении дисциплины «Криптографические методы защиты информации». Освоение дисциплины содержит в себе лекционные, практические и лабораторные занятия, в связи с чем, для комплексного изучения дисциплины необходимо применить структурной подход при реализации данной разработки [5].

Структура учебно-исследовательского комплекса представляет два взаимно независимых блока, реализующие принцип комплексности и гибкости программного средства: блок изучения алгоритма и блок работы с криптографическим алгоритмом. Блок изучения криптографического алгоритма представляет собой совокупность методических данных и рекомендаций, которые направлены на изучение современных криптографических алгоритмов. Данный блок разбивается на определенные разделы, которые утверждены в рабочей программе: теоретический и практический раздел блока данных. Теоретический блок составлен из основных методических материалов, которые позволяют изучить теоретические основы криптографического алгоритма шифрования с описанием используемого математического аппарата. В состав теоретического блока входят следующие разделы:

- теоретические основы алгоритма шифрования;
- методические материалы.

Практический блок составлен из основных методов и приемов, которые используются при закреплении пройденного материала, и более подробного изучения математического аппарата криптографических алгоритмов шифрования. В состав практического блока входят следующие разделы:

- тестовые примеры;
- проверка знаний в виде заданий и тестовых вопросов.

Взаимодействие между теоретическим и практическим блоком, а также их составных компонентов, производится из родительского блока – блока изучения криптографического алгоритма. При необходимости производится выход из алгоритма, через дочерние элементы.

Блок работы с криптографическим алгоритмом предназначен для реализации криптографических шифров и их производных с целью получения практических навыков при работе и взаимодействии с криптосистемой. Структура данного блока строится на принципах синергетического разбиения исходного элемента на более мелкие составные части, которые позволяют реализовать необходимые требования, с высоким уровнем детализации. Результатом синергетического деления криптографического блока являются следующие блоки:

– «слепое» шифрование – режим работы шифрования/ расшифровывания с нулевым уровнем детализации;

– визуализация алгоритма – режим работы программы с максимальным уровнем детализации и активированным режимом интерактивного взаимодействия с пользователем;

– результат работы, блок алгоритма, являющийся производной от предыдущих двух режимов работы алгоритма, определяющий конечный итог проводимых выше действий.

Описанный выше принцип реализации блока работы с криптографическим алгоритмом определяется для каждого алгоритма шифрования (перечень криптографических алгоритмов представлен ниже) который требуется включить в учебно-исследовательский программный комплекс.

В ходе проведенного исследования полученные данные объединяются в единую систему, образуя общую структуру интерактивного программного обеспечения. Разработанная структурная схема алгоритма продемонстрирована на рисунке 1.

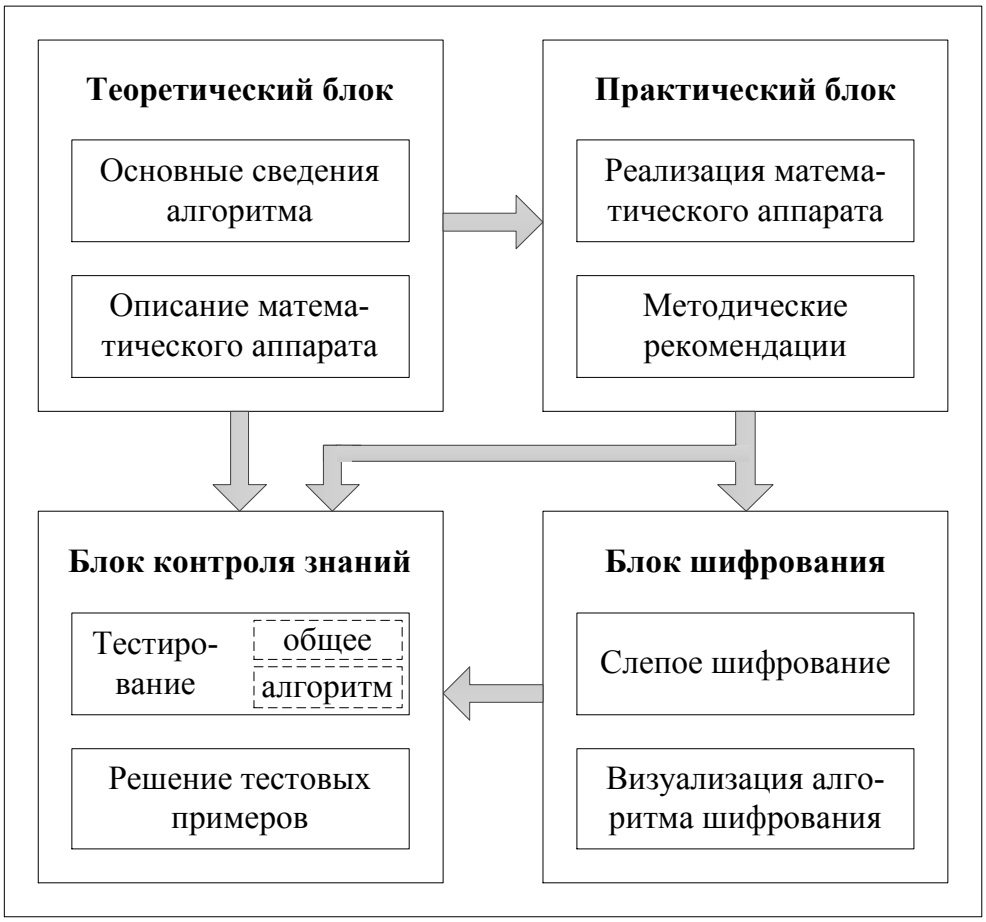

Рисунок 1– Структурная схема учебно-исследовательского комплекса

Структурная схема описывает общий перечень блоков данных, требуемый при реализации данного учебно-исследовательского программного комплекса. Каждый блок реализует приобретение пользователем ряда компетенций в соответствии с требованием ФГОС ВПО по направлению Информационная

безопасность. Для данной структурной схемы был выделен следующий перечень компетенций, приобретаемый при работе с отдельно взятым блоком из структурной схемы, продемонстрирован в таблице 2.

Таблица 2 – Формирование компетенций при работе с интерактивным учебно-исследовательским комплексом построения и анализа шифрования информации

Блок алгоритма программы	Компетенции
Основные сведения алгоритма	ПК-2, ПК-21
Описание математического аппарата	ПК-1, ПК-17, ПК-21
Примеры реализации математического аппарата криптографических алгоритмов	ПК-1, ПК-17
Методические рекомендации к изучению криптографического алгоритма	ПК-1, ПК-2, ПК-17, ПК-21
Тестирование (проверка знаний)	ПК-1, ПК-2
Решение тестовых примеров	ПК-26, ПК-27
Слепое шифрование	ПК-4, ПК-5, ПК-17, ПК-22, ПК-23
Визуализация алгоритма шифрования	ПК-1, ПК-2, ПК-4, ПК-5, ПК-17, ПК-22, ПК-23

Разрабатываемый учебно-исследовательский комплекс способствует формированию перечисленных в таблице профессиональных компетенций для студента по направлению «Информационная безопасность».

Выбор изучаемого алгоритма шифрования предоставляется пользователю системы, что позволяет строить индивидуальные траектории обучения в следующем иерархическом порядке: изучение алгоритма, получение практических навыков работы и проверка полученных знаний и навыков.

Для полноценного процесса обучения, пользователю необходимо предлагать широкий комплекс услуг по изучению криптографических алгоритмов шифрования с возможностью изменения направления по проводимой деятельности. При изучении практических приемов алгоритмов шифрования требуется обеспечить возможность перехода к теоретическому освоению математического аппарата алгоритма с последующей проверкой полученных знаний. Вышеприведенные операции требуется проводить и в обратном направлении для обеспечения всех функций программного комплекса и удобного использования и применения.

Результаты проведенного исследования объединяются в общее представление модели учебно-исследовательского программного комплекса, для представления взаимно связывающихся элементов в модели был выбран сетевой принцип отображения причинно-следственных связей. Принцип работы учебно-исследовательского комплекса показан на рисунке 2.

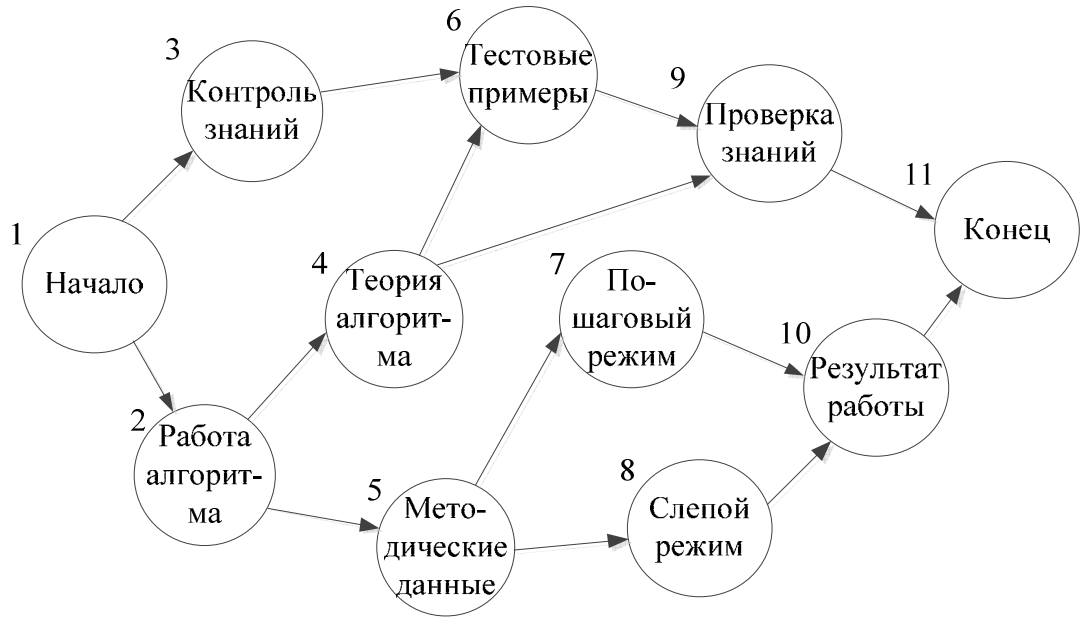

Рисунок 2–Сетевая модель работы интерактивного учебно-исследовательского комплекса построения и анализа алгоритмов шифрования информации

Модель интерактивного учебно-исследовательского программного комплекса, изображенная на рисунке 2 отображает полную концепцию работы программного обеспечения и взаимодействия его основных компонент друг с другом. Взаимодействие большинства элементов производится в обоих направлениях, при котором движение можно производить вверх алгоритма или наоборот. Приведенная схема описывает один цикл работы программного комплекса, последующие шаги программного комплекса производятся аналогично с входом в блоке 1. Перечень реализуемых в комплексе алгоритмов шифрования представлен в таблице 3.

Таблица 3 – Перечень криптографических алгоритмов, реализуемых в учебно-исследовательском программном комплексе

Название шифра	Способ шифрования	Метод шифрования	Актуальность шифра
Шифр Виженера	традиционный (симметричный)	полиалфавитное	не актуален
AES (Rijndael)	симметричный	блочное	актуален
ГОСТ 28147-89	симметричный	блочное	актуален
RC4	симметричный	поточное	актуален
RSA	асимметричный	блочное	актуален

Рассмотренный перечень криптографических алгоритмов представляет необходимый и достаточный минимумом при изучении дисциплины «Криптографические методы защиты информации», и входит в состав разрабатываемого учебно-исследовательского комплекса, который может

применяться в учебном процессе в качестве средства для реализации электронного обучения при самостоятельной работе студентов.

Список литературы

1. Основная образовательная программа высшего профессионального образования. Направление подготовки: 090900 – Информационная безопасность. Профиль подготовки – Комплексная защита объектов информатизации. Квалификация – Бакалавр. Форма обучения – Очная. – Утв. 2011-04-16. – Оренбург: ОГУ, 2011. – 43 с.

2. Рычкова А.А. Разработка и применение прикладных программ учебного назначения для организации самостоятельной работы студентов : сборник научных статей Всероссийской научно-методической конференции «Университетский комплекс как региональный центр образования, науки и культуры»; Оренбургский гос. ун-т. / А.А. Рычкова. – Оренбург: ООО ИПК «Университет», 2014. – С. 3082-3088.

3. Усманов, Р.И. Традиционные симметричные криптографические системы шифрования : Прикладная программа / Р.И. Усманов, А.А. Рычкова – Оренбург: УФЭР. – 2014. - № 916 от 22.01.2014.

4. Усманов, Р.И. Исследование чисел на простоту : Прикладная программа / Р.И. Усманов, А.А. Рычкова – Оренбург: УФЭР. – 2014. - № 917 от 23.01.2014.

Яркова, О.Н. Криптографические методы защиты информации: Рабочая программа дисциплины /О.Н. Яркова. – Оренбург: ОГУ, 2012. - 14 с.