

Министерство просвещения РФ
федеральное государственное бюджетное образовательное
учреждение высшего образования
«Уральский государственный педагогический университет»

Институт математики, физики, информатики
Кафедра информатики, информационных технологий
и методики обучения информатике

ОБУЧЕНИЕ МЕТОДАМ СТРЕГАНОВАГРАФИИ В КУРСЕ ИНФОРМАТИКИ

Выпускная квалификационная работа

Допущено к защите
Зав. кафедрой Сардак Л. В.
«26» мая 2023 г. _____

Исполнитель: Собакина Дарья Ивановна
обучающийся группы МиИ-1801

Руководитель: Стариченко Борис Евгеньевич
доктор педагогических наук,
профессор кафедры ИИТ и МОИ

Екатеринбург – 2023

Оглавление

ВВЕДЕНИЕ	3
ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОБУЧЕНИЯ МЕТОДАМ СТЕГАНОГРАФИИ.....	6
1.1. Место темы «СТЕГАНОГРАФИЯ» В КУРСЕ ИНФОРМАТИКА.....	6
1.2. ТЕХНОЛОГИИ ЦИФРОВОЙ СТЕГАНОГРАФИИ.....	13
1.3. ПРОЕКТИРОВАНИЕ СТРУКТУРЫ И КОНТЕНТА ОТКРЫТОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА «СТЕГАНОГРАФИЯ»	22
ВЫВОДЫ ПО МАТЕРИАЛАМ ГЛАВЫ 1	29
ГЛАВА 2. РЕАЛИЗАЦИЯ ОТКРЫТОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА ПО ТЕМЕ «СТЕГАНОГРАФИЯ».....	30
2.1. ОТКРЫТЫЙ ОБРАЗОВАТЕЛЬНЫЙ РЕСУРС ДЛЯ ИЗУЧЕНИЯ ТЕМЫ «СТЕГАНОГРАФИЯ»	30
2.2. СТЕГАНОГРАФИЧЕСКИЕ ЗАДАЧИ И ПРОЕКТЫ	36
2.3. ОРГАНИЗАЦИЯ ОПЫТНО-ПОИСКОВОЙ РАБОТЫ И ЕЕ РЕЗУЛЬТАТЫ.....	55
ЗАКЛЮЧЕНИЕ	61
ИСТОЧНИКИ ИНФОРМАЦИИ	62

Введение

Стремительный рост информационных технологий приводит к тому, что большая часть информации теперь находится в электронном виде, вместе с тем возрастает сложность обеспечения ее защиты. Сейчас появляется все больше возможностей для несанкционированного доступа к передаваемой информации. Таким образом, угроза нарушения информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

О необходимости изучения элементов информационной безопасности говорится и в Федеральном государственном образовательном стандарте основного общего образования от 31 мая 2021[22]. Так в предметных результатах по учебному предмету «Информатика» на базовом уровне можно выделить следующий пункт: «Умение использовать различные средства защиты от вредоносного программного обеспечения, умение обеспечивать личную безопасность при использовании ресурсов сети Интернет, в том числе умение защищать персональную информацию от несанкционированного доступа и его последствий (разглашения, подмены, утраты данных) с учетом основных технологических и социально-психологических аспектов использования сети Интернет (сетевая анонимность, цифровой след, аутентичность субъектов и ресурсов, опасность вредоносного кода)»[22, стр 83].

В последние годы с развитием цифровых технологий записи и обработки информации появилось направление смежное с криптографией, позволяющее скрывать сам факт передачи информации, под названием стеганография.

Стеганография позволяет решать следующие задачи защиты информации:

- скрытая передача и хранение конфиденциальной информации;
- защита авторских прав на интеллектуальную собственность;
- проверка подлинности и неизменности контейнера;
- преодоление систем мониторинга и управления сетевыми ресурсами;
- камуфлирование программного обеспечения [3, 20].

Элементы стеганографии также рассматриваются и в школьном курсе информатики. Примером этому является учебник: Информатика. Углубленный уровень: для 10 класса: в 2 ч. Ч. 2 / К. Ю. Поляков, Е. А. Еремин [16]. Тема «Стеганография» рассматривается в разделе «Информационная безопасность».

В настоящее время стеганографическая технология не стоит на месте, она продолжает бурно развиваться. В этом направлении публикуются различные статьи, защищаются диссертации, проводятся конференции и многое другое.

На основании сказанного вытекает **актуальность** изучения стеганографии в курсах информатики на различных уровнях обучения.

Проведенный анализ позволяет выделить ряд противоречий:

- *на научно-педагогическом уровне* – между необходимостью изучения стеганографии в курсе информатики и недостаточной развитостью теоретических основ для организации обучения;
- *на научно-методическом уровне* – между потребностью в реализации обучения методам стеганографии и отсутствием методических подходов к его реализации.

Необходимость разрешения перечисленных противоречий обуславливает актуальность данного исследования, а также его **проблему**: каким образом обеспечить обучение стеганографии в курсах информатики разного уровня? В рамках указанной проблемы нами определена **тема исследования**: «Обучение методам стенографии в курсе информатики».

Объект исследования: процесс обучения информатике и информационным технологиям.

Предмет исследования: открытый образовательный ресурс «Стеганография» и варианты его использования в курсе информатики.

Цель исследования: разработать структуру и содержание открытого образовательного ресурса по теме «Стеганография», а также варианты его использования при изучении информатики и информационных технологий.

На основании цели исследования и рабочей гипотезы были поставлены (сформулированы) следующие **задачи исследования**:

1. Произвести анализ библиографических данных, посвященных теме «Стеганография», для обоснования необходимости изучения стеганографии в курсе информатики и построения терминологического аппарата.

2. Проанализировать технологии цифровой стеганографии с точки зрения возможности их освоения в курсе информатики на различных уровнях обучения.

3. Разработать структуру и общее содержание открытого образовательного ресурса «Стеганография».

4. Реализовать открытый образовательный ресурс по теме «Стеганография» с открытой лицензией использования. Разработать комплекты учебных заданий и проектов по изучаемой теме.

5. Осуществить опытно-поисковую работу по оценке разработанного ресурса.

Глава 1. Теоретические основы обучения методам стеганографии

1.1. Место темы «Стеганография» в курсе информатика

Стремительный рост информационных технологий приводит к тому, что большая часть информации теперь находится в электронном виде. Вместе с тем возрастает сложность обеспечения ее защиты. Сейчас появляется все больше возможностей для несанкционированного доступа к передаваемой информации. Таким образом, угроза нарушения информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

Под информационной безопасностью в Российской Федерации (информационной системы) подразумевается «техника защиты информации от преднамеренного или случайного несанкционированного доступа и нанесения тем самым вреда нормальному процессу документооборота и обмена данными в системе, а также хищения, модификации и уничтожения информации» [5].

В.В. Анисимов выделяет следующие методы защиты информации [4]:

- **препятствие на пути предполагаемого похитителя**, которое создают физическими и программными средствами;
- **управление** или оказание воздействия на элементы защищаемой системы;
- **маскировка** или преобразование данных обычно криптографическими способами;
- **регламентация** или разработка нормативно-правовых актов и набора мер, направленных на то, чтобы побудить пользователей, взаимодействующих с базами данных, к должному поведению;
- **принуждение** или создание таких условий, при которых пользователь будет вынужден соблюдать правила обращения с данными;
- **побуждение** или создание условий, которые мотивируют пользователей к должному поведению.

К одним из самых надежных методов защиты информации от несанкционированного доступа, копирования, хищения и искажения можно отнести криптографическое закрытие исходных данных.

Криптография – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации [4].

Методы криптографии реализуются преобразованием информации, которое делает исходные данные нечитаемыми без знания алгоритма и его ключа. Под ключом понимается переменный параметр шифра, обеспечивающий выбор одного преобразования из совокупности всевозможных для данного алгоритма и сообщения.

В современном мире криптографические методы и средства имеют наиболее широкое применение в сфере скрытия и передачи информации как в общественной, так и в личной жизни. При работе за компьютером, использовании смартфона или планшета, получении банковских или государственных услуг используется криптография. При выходе в Интернет используется сразу несколько криптографических протоколов, в то время как обычные пользователи об этом не догадываются.

Согласно Аль-Аммори, «криптография включает в себя несколько разделов современной математики, а также специальные отрасли физики, радиоэлектроники, связи и некоторых других смежных отраслей» [2]. Задачами криптографии являются:

- обеспечение конфиденциальности информации;
- обеспечение целостности информации;
- обеспечение аутентификации;
- обеспечение неотказуемости.

Согласно Б.Е. Стариченко, криптографические методы чаще всего разделяют в зависимости от количества ключей, которые используются в криптоалгоритмах [19]:

- бесключевые – методы, в которых ключи не используются;
- одноключевые – методы, в которых один секретный ключ используется для всех авторизованных пользователей;
- двухключевые – данные методы используют в своих алгоритмах используют два ключа: секретные и открытый.

Исходя из выше сказанного, можно сделать вывод о том, что проблемы защиты информации являются весьма значимыми в современном мире. Они охватывают все стороны деятельности государств, компаний и отдельных людей. В связи с чем появляется необходимость в изучении методов защиты информации на различных ступенях обучения.

О необходимости изучения элементов информационной безопасности говорится и в Федеральном государственном образовательном стандарте основного общего образования от 31 мая 2021[22]. Так, в предметных результатах по учебному предмету «Информатика» на базовом уровне можно выделить следующий пункт: «Умение использовать различные средства защиты от вредоносного программного обеспечения, умение обеспечивать личную безопасность при использовании ресурсов сети Интернет, в том числе умение защищать персональную информацию от несанкционированного доступа и его последствий (разглашения, подмены, утраты данных) с учетом основных технологических и социально-психологических аспектов использования сети Интернет (сетевая анонимность, цифровой след, аутентичность субъектов и ресурсов, опасность вредоносного кода)»[22, стр 83]. На углубленном уровне в предметных результатах по учебному предмету «Информатика» к базовым умениям добавляется умение распознавать попытки и предупреждать вовлечение себя и окружающих в деструктивные и криминальные формы сетевой активности (в том числе кибербуллинг, фишинг) [Там же, стр 86-87].

В последние годы, с развитием цифровых технологий записи и обработки информации, появилось направление, смежное с криптографией, позволяющее скрывать сам факт передачи информации под названием стеганография. При этом информация, подлежащая передачи, размещает во внешнем

информационном контейнере – тексте, изображении, видео и пр. Использование стеганографии в настоящее время становится все более популярным для решения ряда задач. К таким задачам относятся: скрытая передача и хранение разнообразной конфиденциальной информации, включая мультимедийную; защита авторских прав на интеллектуальную собственность (за счет создания цифровых водяных знаков (ЦВЗ)); проверка подлинности и неизменности контейнера; преодоление систем мониторинга и управления сетевыми ресурсами; камуфлирование программного обеспечения [3, 20].

Элементы стеганографии рассматриваются и в школьном курсе информатики. Примером этому является учебник: Информатика. Углубленный уровень: для 10 класса: в 2 ч. Ч. 2 / К. Ю. Поляков, Е. А. Еремин [16]. Тема «Стеганография» рассматривается в разделе «Информационная безопасность». Вопросам стеганографии посвящен один параграф и отводится 1 час. В параграфе рассматриваются определение стеганографии, некоторые некомпьютерные методы стеганографии, а также простейшие программные методы (добавление текста в изображение, методы для звуковых данных и видеоданных), рассказывается о цифровых водяных знаках.

В работе Б.Е. Стариченко и Л.В. Сардак стеганография определяется как наука о методах и механизмах сокрытия факта передачи нужной информации путем ее включения в другое сообщение [20].

Аналогичное определение в своей работе дает В.А. Частикова: «Стеганография - это наука о скрытой передаче информации путем сохранения в тайне самого факта передачи» [24].

В материале «Стеганография в XXI веке» она определена, как междисциплинарная наука и искусство передавать сокрытые данные внутри других, не сокрытых данных [21].

П. В. Слипенчук в своей работе дает следующее определение: «Стеганография – это искусство и наука передавать сообщения различными способами так, чтобы не было обнаружено наличие самого сообщения, это область

знаний о сокрытии информации; это процесс вкрапления представленной в какой-либо форме информации внутрь другой информации» [18].

Все рассмотренные определения передают суть стеганографии, которая заключается в скрытии факта передачи секретного сообщения.

Рассмотрим терминологию стеганографии.

Сообщение, в которое помещается скрытая информация, называют стеганографическим контейнером, а скрываемая информация называется стегосообщением. В свою очередь, контейнер, не содержащий скрытой информации, называют пустым, в противном случае – заполненным (или стегоконтейнером). Контейнером для стегосообщения может служить изображения, аудио- и видеофайлы, а также текстовые документы различных форматов. Для каждого вида контейнера разработаны различные стеганографические методы.

Совокупность методик и средств встраивания и извлечения дополнительной информации без обнаружения нарушения целостности контейнера потребителем позволяет говорить о формировании скрытого (стеганографического) канала передачи информации.

Согласно работе Е.С. Абазина и А.А. Ерунова, в настоящее время выделяют три направления стеганографии: классическая, компьютерная и цифровая [1].

Классическая стеганография включает в себя «некомпьютерные» методы. Примером такой стеганографии является метод симпатических (невидимых) чернил, в этом методе сообщение пишется невидимыми чернилами, которые становятся видимыми при определенных условиях (нагрев, освещение, химический проявитель и т. д.).

Компьютерная стеганография связана с использованием свойств форматов данных, передаваемых и обрабатываемых в инфокоммуникационных сетях. Примером этому может служить запись данных в областях файла, недоступных для обычных приложений.

Цифровая стеганография основана на избыточности пересылаемых мультимедийных данных, представленных в цифровом виде, изначально имеющих аналоговую природу (изображения, видео, звук).

До последнего времени применялась только текстовая стеганография, и ее применение носило весьма ограниченный характер, хотя было разработано большое количество алгоритмов сокрытия передаваемых текстов внутри текстов-контейнеров. Ситуация изменилась вместе с возникновением современных цифровых технологий и связанных с ними задач защиты информации.

В настоящее время стеганографическая наука не стоит на месте, она продолжает бурно развиваться. В этом направлении публикуются различные статьи, защищаются диссертации, проводятся конференции и многое другое.

Развитие и распространение методов стеганографии при решении многих практических задач защиты информации делает актуальным их изучение в курсах информатики различного уровня. Как указывается в работе Б.Е. Стариченко, для при рассмотрении и реализации методов стеганографии могут быть использованы различные подходы:

- инструментальный – использование специализированных приложений и утилит;
- использование приложений общего назначения (текстовые, графические, видео и звуковые редакторы);
- программная реализация стеганографических алгоритмов [20].

Методы и задачи стеганографии могут рассматриваться при освоении пользовательских общих и специализированных приложений, а также при изучении программирования.

Сказанное обуславливает актуальность изучения методов стеганографии в курсах информатики наряду с другими методами защиты информации. Однако создание единой программы изучения стеганографии, а также построение универсального информационного ресурса для курсов информатики разного уровня представляется затруднительным, поскольку различаются их дидактические задачи. Возможным решением является разработка Открытого Образовательного Ресурса (ООР) который включал бы учебные материалы различной направленности и глубины, что позволило бы на основе этого ресурса построить множество учебных курсов для конкретных задач и условий обучения.

ЮНЕСКО предлагает представлять под ООР «обучающие и исследовательские ресурсы, которые находятся в общественном достоянии или выпущены под лицензией на свободную собственность, разрешено их свободное использование или переориентирование для других целей» [27]. Исходя из данного определения, к ООР можно относить учебники, учебные материалы, курсы, видео- и аудиоматериалы, тесты и другие инструменты, материалы или технологии, направленные на обеспечение доступа к знаниям.

Согласно Н.В. Днепровской и И.В. Швецовой [10] определение «ООР» значительно шире, чем «электронные издания», и не налагает ограничений на формат и возможности концентрации. ООР включает в себя электронный курс или учебник, так и отдельные элементы материала пример, презентацию, видеоролик, деловую игру, сценарий урока.

Отличительными особенностями ООР являются:

- методическая, учебная или научная направленность материалов;
- поддержание различных форматов и носителей для представления материалов;
- опубликование на условиях открытой лицензии учебных и научных материалов, являющихся общественным достоянием;
- обеспечение бесплатного доступа, использования, переработки и перераспределения материалов другими пользователями;
- минимальные ограничения либо без таковых при работе с ООР;
- открытое лицензирование встроено в существующую систему прав интеллектуальной собственности, определенных соответствующими международными конвенциями, и признает авторское право на произведение.

Открытые образовательные ресурсы должны отвечать следующим требованиям:

- соответствие современным стандартам;
- удобство создания и сопровождения;
- интерактивность, адаптивность и переносимость;
- доступность и эффективность.

ООР являются цифровыми ресурсами, они могут создаваться с помощью широкого набора информационных технологий и сервисов, включая ведение блога, разработку интеллектуальной карты, видеоматериал, дополненную реальность и так далее.

Целью создания ООР по теме «Стеганография» является обеспечение бесплатного доступа, использования, переработки и перераспределения материалов другими пользователями.

Главной идеей разработки ООР является создание цифрового образовательного ресурса, состоящего из модулей, включающих теоретический и практический материал по теме «Стеганография» подходящих для различного уровня освоения темы, что позволит в дальнейшем построить множество конкретных учебных курсов для разного уровня освоения, в том числе школьного.

Таким образом: представляется актуальным включить изучение темы «Стеганография» в курсы информатики различного уровня, что требует определения содержания и методов обучения технологиям цифровой стеганографии.

1.2. Технологии цифровой стеганографии

Как уже отмечалось, основная идея стеганографии – сокрытие факта наличия и передачи информации. Стеганографические методы защиты информации предназначены для обеспечения конфиденциальности и целостности путем сокрытия информации. Некоторые из них, так называемые цифровые водяные знаки, могут служить для обеспечения целостности, то есть для контроля несанкционированных изменений в информационном объекте. Такие меры защиты информации могут применяться в условиях, когда потенциальный нарушитель является легальным пользователем другого объекта или информации. В этом случае с их помощью обеспечивается защита, к примеру, авторских прав, соблюдение условий лицензии. Например, пользователь получает доступ к электронной книге с ограничением на устройства, с которых он может ее открывать, и ограничением на пересылку ее другим

пользователем. Тогда стенографические методы защита информации могут быть применены для обеспечения контроля и отслеживания попыток расширения круга покупателей данной книги, то есть для пресечения похищения интегральной собственности, нарушения авторского права.

Согласно Е.С. Абазиной и А.А. Ерунову методы цифровой и компьютерной стеганографии в общем виде могут быть классифицированы по целям использования, по виду выбранного контейнера для встраивания, по структуре контейнера [1].

По целям использования методов цифровой и компьютерной стеганографии общепризнанными являются три направления:

- встраивание скрытых каналов передачи информации – цель: сокрытие факта передачи информации;
- встраивание цифровых водяных знаков (ЦВЗ) – цель: подтверждение подлинности передаваемой информации, а также в предотвращении несанкционированного доступа к ней;
- встраивание идентификационных номеров (цифровые отпечатки пальцев) – цель: сокрытие аннотации и аутентификации передаваемых данных [12].

Рассмотрим подробнее два последних метода.

Встраивание ЦВЗ заключается в внедрении в сообщение цифровых отпечатков (digital fingerprints). Это незаметные без специальной обработки скрытые знаки, неповторимые для каждого сообщения. Такие знаки служат для защиты интересов правообладателей и позволяют отследить распространение контента. Основные требования, предъявляемые к водяным знакам: надежность и устойчивость к искажениям, незаметности, робастности к обработке сигналов (робастность – способность системы к восстановлению после воздействия на нее внешних/внутренних искажений, в том числе умышленных). ЦВЗ имеют небольшой объем, но для выполнения указанных выше требований, при их встраивании используются более сложные методы, чем для встраивания обычных заголовков или сообщений. Такие задачи выполняют специальные стегосистемы.

Третье направление изучает методы добавления к сообщению скрытых или стеганографических меток (stegomarks). В отличие от цифровых отпечатков метки, идентичны для всех файлов одного человека или устройства. В данном случае метки применяются для подтверждения авторского права.

По виду контейнера, выбранного для встраивания стеговложений, стеганографические методы разделяют на методы, подвергающие модификации данные и программы, текст, аудио и видео. Организация скрытых вложений в большей степени возможна благодаря избыточности вида данных, который выбран носителем, в связи с этим более популярно применение для этой задачи аудио и видеоданных, как наиболее избыточных.

В соответствии с тем, какая область в структуре контейнера подлежит модификации, различают форматные и неформатные стегометоды. Форматные методы сокрытия включают в себя методы, которые основываются на особенностях формата хранения данных. Применение данных методов ограничено слабой стеганографической стойкостью при довольно низкой пропускной способности и более применимо для организации ЦВЗ. Неформатные методы основываются на модификации параметров пространства сокрытия файла, характеризующих непосредственно данные самого изображения или звука. Это направление является более перспективным и основывается на изменении параметров пространства сокрытия файла, характеризующих непосредственно данные самого изображения или звука. В этой области разработаны, а также хорошо апробированы стойкие к обнаружению стеганографические алгоритмы, которые обеспечивают достаточную емкость контейнеров. Так как скрытая пропускная способность зависит непосредственно от избыточности контейнера, то чаще всего применяются применимыми в интересах организации скрытой передачи информации являются подвижные и неподвижные изображения.

Один из первых методов встраивания стеговложения был основан на замене наименее значащего бита контейнера (НЗБ). Этот метод прост в реа-

лизации и позволяет достичь максимума скрытой пропускной способности, однако обладает наименьшей скрытностью и робастностью.

В работе В. Г. Грибунина [9] в качестве альтернативных методов замены указаны следующие.

Встраивание с помощью инверсии бита, так «1» может соответствовать замена $0 \rightarrow 1$, «0» - замена $1 \rightarrow 0$. Встраивание путем вставки бита непосредственно перед модифицируемым битом, при этом значение бита ЦВЗ должно быть противоположно значению бита контейнера.

Встраивание удалением бита, для этого выбираются пары битов «01» или «10» битов, которые соответствуют разным значениям бита ЦВЗ. Затем первый бит пары удаляется.

Встраивание с использованием бита-флага, суть которого состоит в том, что очередной бит контейнера (неизменяемый) является битом ЦВЗ, указывает инверсия предшествующего бита-флага.

Встраивание с применением пороговых бит: используется бит-флаг, но одному биту ЦВЗ соответствует несколько идущих следом за флагом бит (нечетное число). Если среди этих бит больше единиц, то бит ЦВЗ равен «1». Встраивание с использованием табличных значений. Для определения бита ЦВЗ в предыдущем методе, фактически, использовалась проверка на четность. С тем же успехом можно было бы применять и любое другое отображение множества бит в 1 бит, либо находить его значение по таблице. Возможно использование динамически изменяемой таблицы, когда она изменяется на каждом шаге или выбор значения осуществляется псевдослучайно. Так как табличные значения (биты контейнера) знает и кодер, и декодер, то их можно не передавать (косвенная динамическая таблица).

Встраивание с применением функции, оценивающей статистику изображение и корреляционные связи между элементами изображения, и последующее применение этой функции для каждого элемента изображения для определения стегопути. При этом в качестве функции может быть использована псевдослучайная последовательность (ПСП).

Другим подходом, отличным от первых двух, является встраивание дополнительной информации за счет энергетической разницы между коэффициентами контейнера, характеризующееся малым изменением статистики изображения.

В цифровой стеганографии также применяются метод LSB, эхо-методы, фазовое кодирование, метод расширенного спектра.

Метод LSB – суть этого метода заключается в замене последних значащих битов в контейнере (изображения, аудио или видеозаписи) на биты скрываемого сообщения. Разница между исходным файлом и заполненным контейнером должна быть незаметна для восприятия человека

Эхо-методы используются в цифровой аудиостеганографии. Для скрытия последовательности значений используют различные промежутки между эхо-сигналами. Для незаметности изменений для человеческого восприятия необходимо соблюдать ряд ограничений. Эхо характеризуется тремя параметрами: начальной амплитудой, степенью затухания, задержкой. Что бы человеческое ухо не могло отличить сигнал и эхо, они смешиваются путем достижения некоторого порога между ними. При обозначении логического нуля и единицы используют две различные задержки, которые должны быть меньше порога чувствительности уха слушателя.

Фазовое кодирование еще один метод применяемый в цифровой аудиостеганографии. В данном методе исходный звуковой элемент заменяют на относительную фазу, которая является секретным сообщением. Фаза подряд идущих элементов добавляется таким образом, чтобы сохранить относительную фазу между исходными элементами. Данный метод относится к одним из самых методов сокрытия информации.

Метод расширенного спектра – специальная последовательность встраивается в контейнер, после чего эта последовательность детектируется с помощью согласованного фильтра. При использовании данного метода можно встраивать большое количество информации в контейнер, при это они не будут создавать друг другу помехи.

Среди текстовых методов стеганографии Н.П. Шутько выделяет модификацию цветовых параметров и модификацию апроша и кернинга [26].

Модификация цветовых параметров основана на изменении цвета пикселей, формирующих символы текста, их можно изменить так, что это остается незаметным для других лиц в силу специфики человеческого зрения. Формально рассматриваем текстовый документ-контейнер как графический объект. В этом и других методах в качестве базового элемента контейнера, свойства которого модифицируются при осаждении информации, выступает символ текста, включая пробел.

Алгоритмы реализации методов модификацию апроша и кернинга в большинстве своем схожи с методом изменения цветовых параметров. Однако имеются в каждом случае свои особенности. Так, метод изменения кернинга можно реализовать двумя способами:

1. Осаждение информации производится за счет изменения значения кернинга любого символа в документе-контейнере.

2. Первоначально проводится анализ документа-контейнера на наличие в нем кернинговых пар. Существует таблица кернинговых пар для каждого семейства шрифтов. В ней приводятся те самые особые пары символов. Предполагается осаждать информацию за счет изменения значения кернинга именно между такими парами символов.

Как отмечалось ранее можно выделить три основных подхода к решению задач цифровой стеганографии:

- инструментальный – использование специализированных приложений и утилит;
- с помощью приложений общего назначения (текстовые, графические, видео- и звуковые редакторы);
- программная реализация стеганографических алгоритмов.

Рассмотрим подробнее каждый из подходов.

Для стеганографии существует множество специализированных приложений и утилит. Приведем примеры самых распространенных из них.

ImageSpyer G2 – утилита позволяющая скрывать информацию в графических файлах с помощью методов стеганографии, а также использует шифрование данных двухслойной криптографической защитой. Поддерживается около тридцати алгоритмов шифрования, а также двадцати пяти хеш-функций для шифрования контейнера. Таким образом механизмы, применяемые в программе ориентированы не только на скрытие информации, но и на то чтобы защитить ее от потенциальных атак [33].

RedJPEG – программа направлена на скрытие любых данных в JPEG изображении, фото или картинке с помощью авторского стеганографического метода. Для внедрения данных в изображение применяются открытые алгоритмы шифрования и мощная LZMA компрессия. Изображение меняется незначительно, без искажений. Визуально модификацию практически не различить [36].

DarkCryptTC – это мощное стеганографическое решение. Является продолжением разработок ImageSpyer и StegoTC и реализует алгоритм LSB, используя в качестве: контейнера для зашифрованных архивов изображения PNG, BMP, TIFF, PSD, TGA, MGA, аудиофайлы, WAVE, текстовые, XML и HTML файлы (текстовая стеганография, алгоритм замены символов) [30].

OpenStego проект реализован на языке Java и имеет поддержку шифрования AES. Помимо этого, также поддерживаются плагины, позволяющие пользователю самому реализовать какой-либо сам стеганографический алгоритм. Имеются версии программы для Windows и для Linux. Имеется возможность крывать данные практически любого формата, однако контейнер может быть только в формате PNG. Как и ImageSpyer, OpenStego значительно раздувает размеры файла [35].

DeepSound распространяется бесплатно и позволяет скрывать информацию в аудиофайлах с форматами FLAC, APE и WAV. Также есть возможность добавления пароля к зашифрованным файлам. Особенностью программы является весьма информативный интерфейс и возможность сокрытия файлов довольно больших объемов [31].

Steganos Privacy Suite представляет собой комплекс приложений для защиты информации. Для стеганографии используется модуль Crypt & Hide, позволяющий скрывать данные в изображениях, музыкальных и видеофайлах. При этом производится дополнительное шифрование по 384-разрядному алгоритму AES-XEX [37].

StegoStick – программа с открытым исходным кодом, позволяющая скрывать любые файлы в JPG, GIF, BMP, AVI, WAV и другие типы файлов. Имеется возможность один из четырех предложенных методов шифрования, а именно DES, Triple DES, RSA [38].

В табл.1. проведено сопоставление характеристик данных приложений и утилит.

Таблица 1

Стеганографические приложения и утилиты

	платно / бесплатно	Входные форматы файлов	Выходные форматы файлов (контейнер)
ImageSpyer G2	Бесплатно	Текстовые, графические, аудио и видео	BMP, TIFF
RedJPEG	Бесплатно	Текстовые, графические, аудио и видео	JPEG
DarkCryptTC	Бесплатно	Текстовые, графические, аудио и видео	PNG, BMP, TIFF, PSD, TGA, MGA, аудиофайлы, WAVE, текстовые, XML и HTML.
OpenStego	Бесплатно	Графические, текстовые	PNG
DeepSound	Бесплатно	FLAC, APE и WAV	FLAC, WAV
Steganos Privacy Suite	Условно-бесплатно (есть пробный период)	Текстовые, графические, аудио и видео	Графические, аудио и видео
<u>StegoStick</u>	Бесплатно	Текстовые, графические, аудио и видео	Графические, аудио и видео

Рассмотренные системы стеганографии не требуют углубленных знаний стеганографии. Большинство из них распространяются абсолютно бесплатно, что является преимуществом при обучении стеганографии. Многие приложения и утилиты позволяют совместно с методами стеганографии использовать криптографические методы, что дает возможность более надежно защищать информацию. Данные программы являются одними из самых рас-

пространенных, однако существует большое количество программ, не попавших в этот список.

Согласно Б.Е. Стариченко и Л.В. Сардак при использовании стандартных приложений возможно решение следующих задач:

- размещение текста в графическом контейнере с помощью PhotoShop;
- создание цифровых водяных знаков в PhotoShop;
- выявление ЦВЗ и скрытых текстов в файле-изображении;
- использование MS Word для сокрытия текстов [20].

Создание цифровых водяных знаков в PhotoShop производится с помощью инструмента «Текст», форматирования данного текста и регулировки параметра «Непрозрачность».

Для сокрытия текста в MS Word можно использовать метод микроточки или форматирование символов, т.е. изменение цвета символов, цвета фона, размера шрифта, масштаба шрифта или межсимвольного интервала.

Наконец, можно привести примеры задач, решаемых с использованием сред программирования:

- разработать программу, добавляющую ASCII-код одного знака текста к RGB-кодам пикселя и сохраняющую файл в графическом формате с последующей возможностью извлечения скрытой информации;
- разработать программу, реализующую алгоритм LSB с двумя последними битами цвета с маскировкой расположения измененных пикселей;
- на языке VBA разработать программу, скрывающую текст в текстовом файле MS Word (например, за счет незначительного изменения размеров букв, их цвета или интервала между словами контейнера) [20].

В настоящее время компьютерная стеганография продолжает совершенствоваться и развиваться: формируется теоретическая база, ведется разработка новых, наиболее стойких методов встраивания сообщений, появляется все больше программ. Так уже сейчас существуют приложения для стеганографии не только для компьютеров, но и для телефонов. Примерами таких приложений являются Pixelknot и NoClue.

Таким образом: выделяется три основных подхода к решению задач цифровой стеганографии: инструментальный, программный и с помощью приложений общего назначения, что позволяет использовать их при изучении различных разделов курса информатики и в проектной деятельности учащихся; это определяет актуальность разработки облачного электронного ресурса по теме «Стеганография», а также методов ее изучения.

1.3. Проектирование структуры и контента открытого образовательного ресурса «Стеганография»

Одним из основных компонентов определения открытых образовательных ресурсов является следующий тезис: ООР должны быть размещены в свободном доступе либо выпущены под лицензией, разрешающей их свободное использование и модификацию.

Проекты открытого образования дают возможность абсолютно бесплатного доступа к качественным образовательным ресурсам, находящимся в сети, и, таким образом, несомненно, способствуют расширению участия ООР в образовании и дальнейшему продвижению образования.

Предполагается, что разработанный ООР может быть использован как обучающимся для самостоятельного изучения темы на интересующем его уровне, так и преподавателями для формирования курсов по теме «Стеганография». Исходя из этого, можно выделить следующие принципы построения ООР:

- *модульность* предполагает разбиение курса на автономные и целостные модули, т.е. модули не зависят друг от друга и предполагают полное их прохождение;
- *расширяемость контента* выражается в возможности дополнения и развития содержания модулей;
- *облачное размещение* предполагает доступность материала т.е. возможность использовать ресурс различными пользователями в любое время и с любого устройства;

- *полнота охвата по содержанию и методам* ресурс должен содержать достаточно полный и подробный материал и включать рассмотрение различных технологий;
- *гибкость использования* ресурс может использоваться как для самообразования, так и для построения преподавателем отдельного курса или включения в качестве раздела в курс информатики.

Как уже отмечалось, разработанный ресурс должен состоять из модулей. Модульное обучение предполагает такую организацию обучения, при котором обучающийся сам оперирует учебным содержанием.

Согласно Л.Н. Буйлова [8], модуль является автономной структурной частью и имеет:

- более детальную цель;
- дидактические задачи, которым соответствует принципиально важная учебная информация;
- нацеленность на конкретные результаты обучения и четко сформулированные критерии оценки;
- сопровождается контролем знаний и умений, обучающихся на выходе;
- может рассматриваться как самостоятельная программа и вместе с тем как одна из частей, например, модульной, сетевой или разноуровневой дополнительной общеразвивающей программы.

Модули могут быть **инвариантными** (обязательными для изучения) и **вариативными** (обязательными по выбору и не обязательными по выбору).

ООР предполагает использование как для самостоятельного обучения, так и для формирования курсов различных уровней. Для реализации поставленной цели модули должны быть универсальны и позволять пользователю самостоятельно выбирать содержание обучения.

Исходя из методов и подходов к решению задач стеганографии, которые были рассмотрены в предыдущем параграфе, для ООР по теме «Стеганография» можно выделить четыре основных модуля, а также целесообразно добавить два организационных дополнительных модуля:

- *введение в стеганографию* – модуль, содержащий базовые понятия и знания по теме стеганография;
- *стеганография в специализированных приложениях* – в данном модуле будет представлена информация о некоторых методах и стеганографических приложениях, а также по работе с ними;
- *стеганография в пользовательских приложениях* – информация о стеганографических методах, которые можно реализовать с помощью стандартных приложений;
- *программирование стеганографических методов* – модуль, содержащий информацию о стеганографических методах и их реализация на языке программирования Python;
- *задачи по реализации методов стеганографии* – модуль, состоящий из отдельных заданий, которые могут применяться в курсе информатики;
- *стеганографические проекты* – данный модуль содержит возможные темы для проектов, которые можно реализовать в результате прохождения курсов.

На рис. 1 представлена структура ООР.

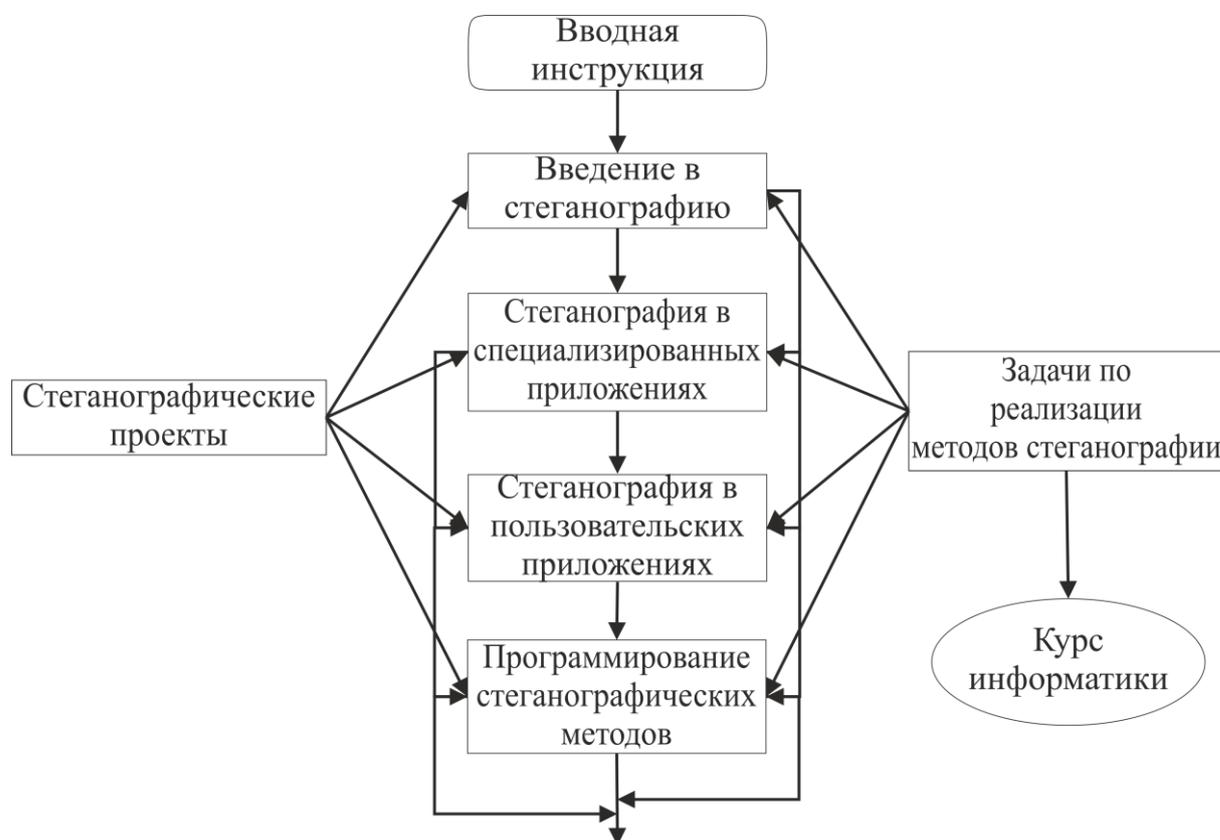


Рис. 1. Структура ООР

В свою очередь, модули состоят из нескольких взаимосвязанных и логически выстроенных элементов (рис. 2). Элементы можно условно разделить на блоки следующих направленностей (рис. 3):

- *теоретический* данный блок может включать тексты, графику, видео, ссылки и др. электронные учебные материалы и электронные образовательные ресурсы;
- *практический*: тексты, видео и др. материалы, посвященные выполнению практических заданий, а также задания для самостоятельной работы (задания для составления практической части курса по теме «Стеганография»);
- *блок контроля* усвоения теории и алгоритмов с отсылкой (при необходимости) к повторному прохождению элемента.

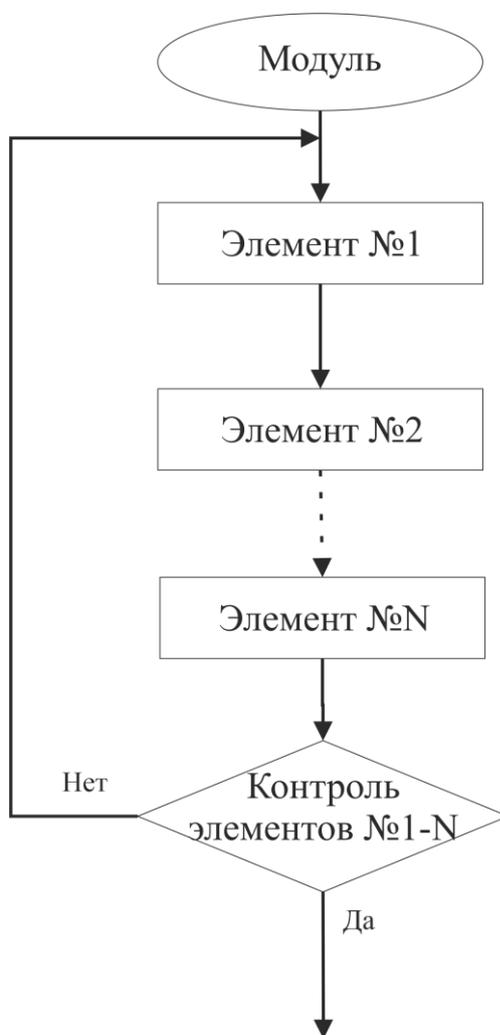


Рис. 2. Структура модуля

После изучения каждого модуля обязательно производится контроль усвоения материала. При неудовлетворительном прохождении контроля да-

ются рекомендации по устранению ошибок, делаются отсылки к материалу, который необходимо повторить, а также производится повторное изучение неувоенного материала с последующим контролем усвоения. В практическом блоке так же содержатся задания, при неправильном выполнении которых предлагается повторить теоретический блок.

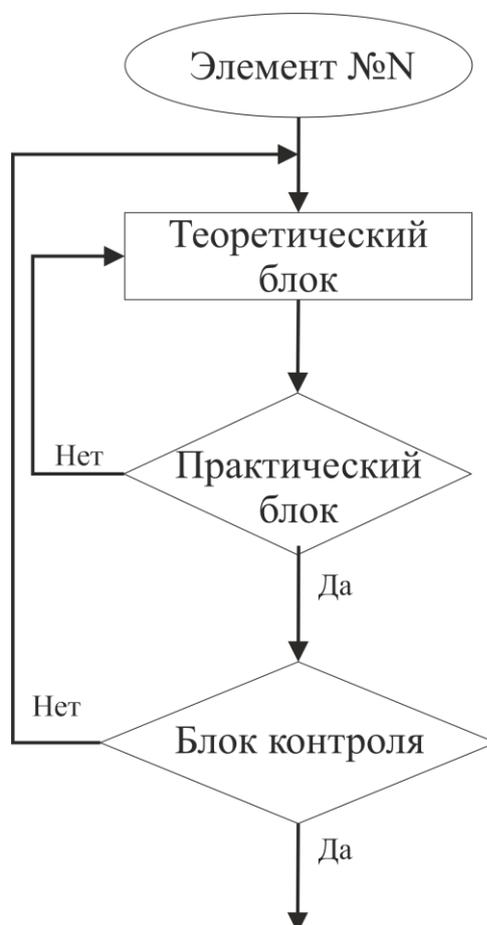


Рис. 3. Структура элемента

Как уже отмечалось, разработанный ООР может применяться как для самостоятельного обучения, так и в помощь педагогам для построения отдельных курсов или разделов курса.

При самостоятельном обучении может быть несколько вариантов работы с сервисом:

- изучение отдельных тем, интересующих обучающегося – данный вариант подойдет тем, кто хочет повторить или уточнить уже имеющиеся знания по стеганографии, а также тем, кто хочет изучить тему на определенном уровне;
- последовательное изучение всех элементов – дает полное погружение в тему;

- выбор траектории обучения – обучающийся выбирает модули и темы, которые хочет изучить, выстраивает последовательность их изучения (в этом варианте при отсутствии базовых знаний по теме рекомендуется начинать обучение с модуля «Введение»).

Для создания курсов на основе ООР можно выделить несколько этапов:

1. Выявление уровня знаний обучающихся.
2. Определение цели и задачи обучения.
3. Выбор содержания модуля (модулей) ООР исходя из цели и задач обучения.
4. Выбор отдельных элементов, удовлетворяющих потребностям планируемого курса.
5. Формирование курса на основе выбранных элементов.

На основе данного плана была разработана схема рис. 4.

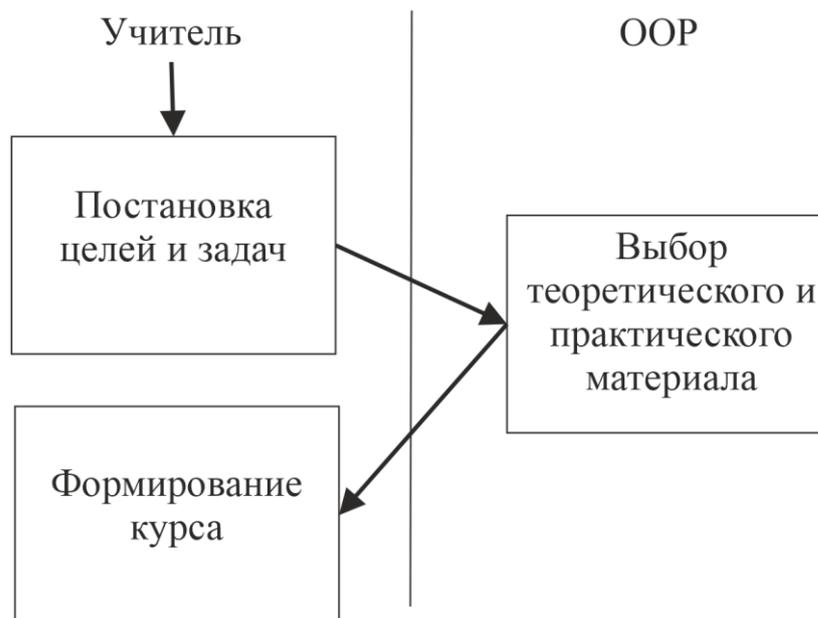


Рис. 4. Создание курсов на основе ООР

Рассмотрим пример планирования изучения темы «Стеганография» на основе описанного ООР для школьного курса информатики по программе Полякова [16].

Уровень знаний обучающихся: Курс рассчитан на обучающихся 10 классов. До этого в школьном курсе не встречается тема «Стеганография».

Цель изучения курса: базовое ознакомление с темой «Стеганография».

Задачи:

1. Ввести определение стеганографии;
2. Рассмотреть краткую историю появления стеганографии;
3. Ознакомиться с некомпьютерными примитивными методами стеганографии;
4. Ознакомиться с базовыми компьютерными методами стеганографии.

Поставленные цели и задачи удовлетворяют содержанию модуля «Введение», следовательно, для разработки данного курса потребуется обратиться к элементам данного модуля.

Приведем пример факультативного курса для вузов «Основы компьютерной стеганографии».

Уровень знаний обучающихся: Курс рассчитан на студентов. Уровень их знаний в области стеганографии может различаться.

Целью освоения дисциплины является овладение основным математическим аппаратом, получение знаний и освоение основных принципов, применяемых в компьютерной стеганографии.

Задачи изучения дисциплины:

1. Изучение основ защиты информации, понятия и методов стеганографии;
2. Формирование умения ориентироваться в современных методах встраивания информации;
3. Владение построениями стеганографических систем.

Курс подразумевает знакомство с понятием стеганографии ее методами и различными подходами. Помимо этого, будут проводиться практические занятия, которые будут включать задания пользовательского уровня. Исходя из этих рассуждений при формировании курса понадобится обратиться к элементам пяти модулей «Введение», «Использование стеганографических приложений», «Использование стандартных приложений», «Программирование» и «Проекты».

Таким образом: предложенные структура и общее содержание ООР «Стеганография» позволят использовать ресурс для создания учебных кур-

сов, ориентированных на решение различных задач обучения; практическая реализация ООР требует разработки конкретного содержания модулей и их размещения в открытом доступе для пользователей.

Выводы по материалам главы 1

1. Представляется актуальным включить изучение темы «Стеганография» в курсы информатики различного уровня, что требует определения содержания и методов обучения технологиям цифровой стеганографии.

2. Выделяется три основных подхода к решению задач цифровой стеганографии: инструментальный, программный и с помощью приложений общего назначения, что позволяет использовать их при изучении различных разделов курса информатики и в проектной деятельности учащихся; это определяет актуальность разработки облачного электронного ресурса по теме «Стеганография», а также методов ее изучения.

3. Предложенные структура и общее содержание ООР «Стеганография» позволят использовать ресурс для создания учебных курсов, ориентированных на решение различных задач обучения; практическая реализация ООР требует разработки конкретного содержания модулей и их размещения в открытом доступе для пользователей.

Глава 2. Реализация открытого образовательного ресурса по теме «Стеганография»

2.1. Открытый образовательный ресурс для изучения темы «Стеганография»

Одной из отличительных особенностей открытых образовательных ресурсов является использование *открытой лицензии* на применение материалов ресурса, допускающей копирование, распространение, модификацию и перевод ресурсов на другие языки, а также их использование для разработки новых образовательных ресурсов.

Одной из компаний, занимающихся лицензиями, является Creative Commons [29]. Бесплатные лицензии, разработанные данной компанией, позволяют автору ограничить права, которые он хочет предоставить другим людям, желающих использовать его продукт. Лицензии данной компании основаны на четырех элементах (табл. 2).

Таблица 2

Элементы лицензии Creative Commons

Название элемента	Русский перевод названия	Символьное обозначение	Графическое обозначение	Пояснение
Attribution	Атрибуция	BY		Требование указывать автора произведения
NonCommercial	Некоммерческое использование	NC		Запрет на использование произведения в целях получения прибыли
NoDerivs	Без производных произведений	ND		Запрет создавать производные произведения
ShareAlike	С сохранением условий	SA		Требование распространять производные произведения только на условиях лицензии исходного произведения

При выборе лицензии для ООР по теме «Стеганография», были поставлены следующие критерии:

- предоставление возможности брать за основу разработанный ресурс и распространять получившийся результат только на условиях лицензии исходного произведения;
- запрет на использование материалов ресурса в коммерческих целях.

Исходя из данных условий была выбрана лицензия Attribution – NonCommercial – ShareAlike, представленная на рис. 5.



Рис. 5. Лицензия Creative Commons

Поскольку предполагается, что к ООР будут иметь доступ многие пользователи, для его размещения требуется облачная платформа. Для ее выбора было проведено сопоставление нескольких платформ.

1. Google Classroom – интернет-сервис для онлайн-обучения. Позволяет создавать курсы, проводить вебинары и тестировать учеников [32].

2. Moodle [34] – популярная система дистанционного обучения (СДО). Ее успешно используют крупные университеты мира, школы и частные компании.

3. CoreApp [28] – онлайн-платформа для запуска курсов, которая разработана для создания, совершенствования и эффективной передачи образовательных материалов.

Результаты сопоставления по нескольким пользовательским характеристикам представлены в табл. 3.

Таблица 3

Анализ онлайн платформ

Критерии	Google Classroom	Moodle	CoreApp
Тарифы	В бесплатной версии можно обучать до 200 студентов в день. Если у вас больше учеников, приобретается подписка. Цены начинаются от 3\$ за ученика в год	От 118 руб/мес	Базовый (0 руб/мес) Профи (990 руб/мес) Гуру (14 000 руб/мес)

Поддержка русского языка	+	+	+
Мобильное приложение	+	+	-
Возможности	<p>Есть редактор курсов, но эти курсы больше похожи на электронные учебники — нет интерактива;</p> <p>Для тестирования и проверки знаний используются google-формы;</p> <p>На этой платформе не проводятся вебинары, но можно провести видеовстречи Google Meet. Есть возможность планировать их в календаре</p>	<p>Настраивать функционал и дизайн сервиса с помощью модулей или плагинов;</p> <p>Есть интеграция с другими сервисами — платформу можно объединить с другими программами, например с вебинарной комнатой Zoom;</p> <p>Создавать текстовые уроки и опросы. Для разработки более качественных уроков, лучше воспользоваться сторонними редакторами курсов;</p> <p>Возможности по управлению пользователями и отчетами зависят от установленных плагинов</p>	<p>Настраивать функционал и дизайн сервиса с помощью модулей;</p> <p>Возможность создавать уроки по шаблонам, добавлять практические упражнения с автоматической и ручной проверкой, создавать интерактивные элементы;</p> <p>Проводить Live-уроки в виде планерок и прямые трансляции. Есть интеграция с Zoom;</p> <p>Выгружать аналитику по результатам обучения</p>

Платформа для разработки ООР должна обеспечивать доступ к материалам в любое время и с любого устройства, быть удобной, а также доступной для всех. Проанализировав таблицу, можно заметить, что Google Classroom больше всего удовлетворяет этим требованиям. Для доступа к этой платформе необходим только Google аккаунт. Имеется мобильное приложение и возможность регулярного обновления и дополнения контента. Платформа объединяет в себе Google Drive, Google Docs, Sheets and Slides и Gmail. Кроме того, сюда интегрирован Календарь и есть возможность делиться видео с платформы YouTube.

В соответствии с принципами и подходами, которые обсуждались ранее в п. 1.3., было осуществлено планирование содержания модулей ООР (табл. 4).

Планирование содержания ООР по стеганографии

Модуль	Элементы
1. Введение в стеганографию	Термины и определения
	История стеганографии. Цифровая стеганография
	Понятие и виды контейнеров
	Направления применения стеганографии
	Текстовые методы стеганографии
	Графические методы стеганографии
	Аудиостеганография
2. Стеганография в пользовательских приложениях	Возможности стеганографии в пользовательских приложениях
	Сокрытие данных в текстовых документах
	Сокрытие данных в изображениях
	Использование метаданных для ЦВЗ
3. Стеганография в специализированных приложениях	Обзор стеганографических приложений
	Сокрытие данных в изображениях
	Сокрытие данных в аудиофайлах
	Сокрытие данных в видеофайлах
4. Программирование стеганографических методов	Программная реализация алгоритмов стеганографии
	Сокрытие информации в текстовом носителе
	Сокрытие информации в изображении
	Сокрытие информации в аудио
Задачи по реализации методов стеганографии	Использование текстовых редакторов для сокрытия информации
	Использование графических редакторов для сокрытия информации
	Сокрытие данных в стегоприложениях
	Программная реализация методов стеганографии
	Олимпиадные задания
Стеганографические проекты	Стеганография в пользовательских приложениях
	Стеганография в специализированных приложениях
	Программирование стеганографических методов

На титульной части ресурса размещена выбранная ранее лицензия Creative Commons (рис. 6).



Рис. 6. Титульная часть ресурса

В разработанной структуре ресурса выделяется шесть модулей: четыре из которых основные, а два других – дополнительные (рис. 7). Основные модули пронумерованы, а дополнительные стоят после основных и не чем не выднляются.

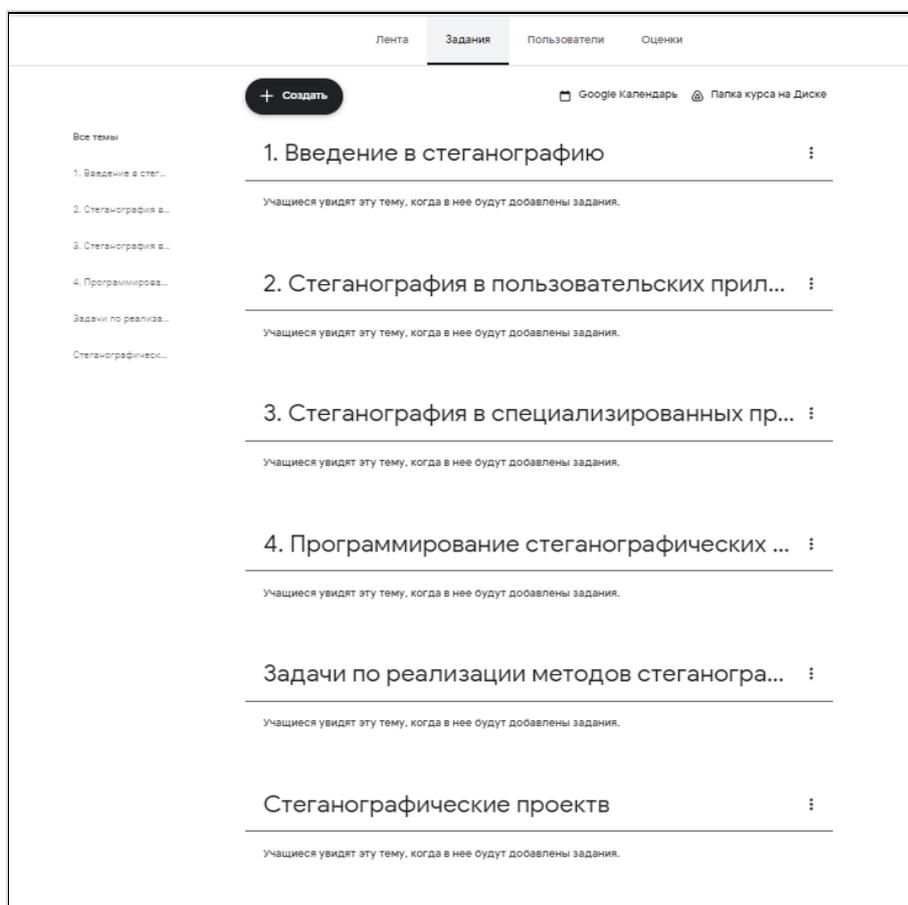


Рис. 7. Модульная структура ООР «Стеганография»

Каждый модуль состоит из учебных элементов (рис. 8). В конце каждого модуля находится блок контроля.

1. Введение в стеганографию		⋮
	Термины и определения	Изменено: 24 апр.
	История стеганографии. Цифровая стеган...	Изменено: 24 апр.
	Понятие и виды контейнеров	Изменено: 24 апр.
	Направления применения стеганографии	Изменено: 24 апр.
	Текстовые методы стеганографии	Опубликовано 16:15
	Графические методы стеганографии	Опубликовано 16:07
	Аудиостеганография	Опубликовано 16:19
	Контрольная работа "Ведение в стеганог..."	Изменено: 24 апр.

Рис. 8. Пример учебного модуля

Каждый учебный элемент содержит в себе теоретическую и практическую части (рис. 9).



Соккрытие данных в изображении

⋮

Дарья Собакина • 13 апр. (Изменено: 16:31)

Ознакомьтесь с представленными документами.
Создайте свой водяной знак и попробуйте самостоятельно добавить его на изображение.
Выполните соккрытие изображении в графическом контейнере.



Размещение изображений ...
PDF



Создание и обнаружение ц...
PDF



Hackerdom-04-08 Цифров...
Видео YouTube 4 минуты

Рис. 9. Пример учебного элемента

Для организации контроля усвоения теоретического и практического материала использовались Google Forms (рис. 10).

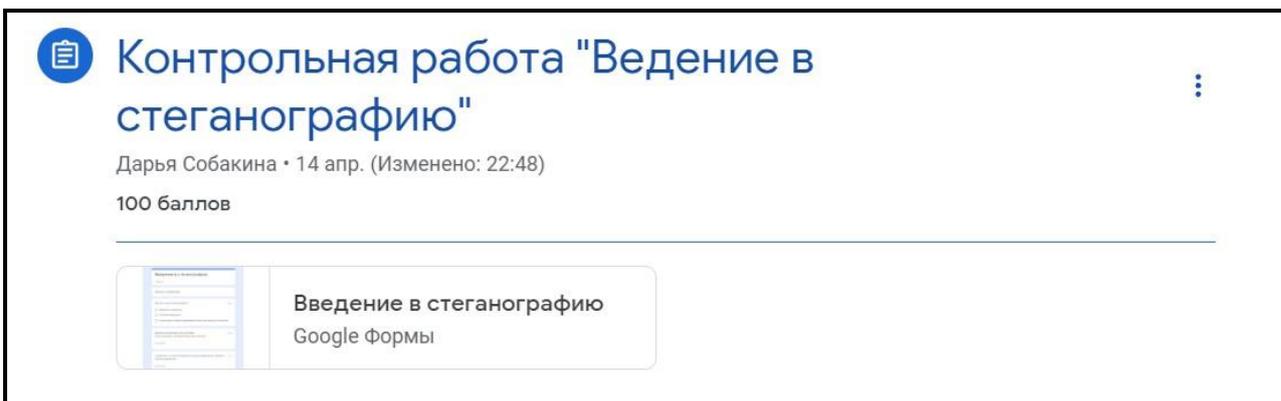


Рис. 10. Пример блока контроля

При наполнении учебных элементов материалом использовались текстовые документы, видео с YouTube, а также различные теоретические и практические задания.

Таким образом, на основании указанных ранее принципов и структуры ресурса был реализован открытый образовательный ресурс с лицензией Creative Commons (Attribution – NonCommercial – ShareAlike).

2.2. Стеганографические задачи и проекты

Два дополнительных модуля содержат примеры задач, которые можно применять в школьном курсе информатики при изучении различных тем, а также примеры проектов, которые можно реализовать в результате прохождения курсов по стеганографии.

Модуль «Задачи по реализации методов стеганографии» включает себя следующие разделы:

1. Сокрытие данных с использованием текстовых редакторов.
2. Сокрытие данных с использованием графических редакторов.
3. Сокрытие данных в стегоприложениях.
4. Программная реализация методов стеганографии.
5. Олимпиадные задания.

Раздел 1.

В разделе содержится задания по реализации методов стеганографии в приложениях MS Word, Яндекс документы, LibreOffice и др.

Первые четыре задания, связанные с форматированием символов текстового документа. Рассмотрим подробно пример решения такого задания в Word.

Задание 1.

Дан текстовый документ. Попробуйте спрятать слово в данном документе, меняя цвет символов.

Важно! Измененные символы не должны бросаться в глаза. Выберете цвет близкий к оригинальному.

Решение:

Дан текстовый контейнер: «Стеганография – это наука о скрытой передаче информации путем сохранения в тайне самого факта передачи». Сообщение: «Секрет». Вторим его в контейнер при помощи замены цвета.

Для этого используем два схожих по оттенку цвета. Для этого в поле шрифт выбираем Цвет текста > Другие цвета > Спектр. Изменяем значения RGB цветов на схожие (рис. 11).

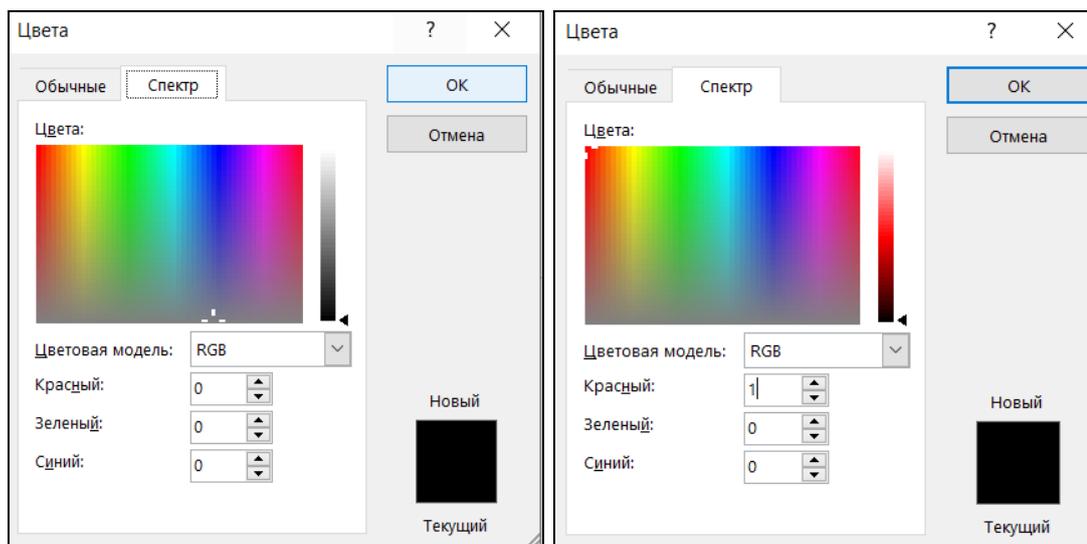


Рис. 11. Вариант изменения цвета

Получаем заполненный контейнер:

«Стеганография – это наука о скрытой передаче информации путем сохранения в тайне самого факта передачи».

Разница в цветах незаметна человеческому взгляду. Для нахождения скрытого сообщения воспользуемся поиском текста в документе. Открываем «Расширенный поиск» в поле Найти выбираем специальный символ «Любая буква» или «^\$». Выбираем Формат > Шрифт. Далее есть два варианта. Если

известен точный цвет закодированных символов, то выбираем его и находим скрытые символы. Если цвет не известен, то выбираем общий цвет обычных символов и перебираем каждую букву.

Следующие три задания также связаны с форматированием документа.

Задание 2.

Дан текстовый документ. Попробуйте спрятать слово в данном документе меняя размер символов.

Важно! Измененные символы не должны бросаться в глаза. Выберете размер близкий к оригинальному.

Задание 3.

Дан текстовый документ. Попробуйте спрятать слово в данном документе меняя цвет фона у символов.

Важно! Измененные фона не должны бросаться в глаза. Выберете цвет близкий к оригинальному.

Задание 4.

Дан текстовый документ. Попробуйте спрятать слово в данном документе заменяя пробелы на символы идентичные по цвету фону.

Данные задания можно применить на уроках информатики в 5-6 классах при изучении темы «Форматирование текстового документа».

Пятое задание требует знаний о системах счисления и представлении данных в компьютере. Его можно применить при изучении темы «Системы счисления». Рассмотрим подробно пример решения такого задания в Word.

Задание 5.

Соккрытие данных в тексте с помощью алгоритма замены символов

Алгоритм замены символов основан на одинаковых в написании буквах английского и русского алфавитов. Отличия таких букв может обнаружить только компьютер.

Каждый символ кодируется определенном двоичным кодом. Для определения этих кодов есть табличка ASCII, любой десятичный номер буквы в этой таблице можно представить в двоичном формате. Например, английская буква k имеет десятичный номер 107, а если перевести эту десятичную циф-

В результате получаем заполненный контейнер:

«Стеганография – это наука о скрытой передаче информации путем сохранения в тайне самого факта передачи».

Для дешифровки можно также воспользоваться расширенным поиском.

Раздел 2.

Данный раздел включает задания на сокрытие данных при помощи графических редакторов.

Первое задание можно выполнить в любом графическом редакторе, оно применимо на уроках в 5-6 классах при изучении графических редакторов. Рассмотрим подробно пример решения такого задания в Paint.

Задание 1

Необходимо создать однотонную картинку, в которой будет скрыт текст.

Примечание! Используйте для текста и фона максимально близкие по оттенкам цвета.

Решение:

Сообщение: «Vas266». Вторим его в контейнер при помощи замены цвета. Для этого используем два схожих по оттенку цвета.

Создаем новое изображение выбираем цвет фона. Для этого вытираем «Изменение цветов», и в открывшемся окне выбираем значения Красного Зеленого и Синего заливаем фон полученным цветом. Далее меняем цвет на близкий к цвету фона с помощью тех же настроек (рис. 13).

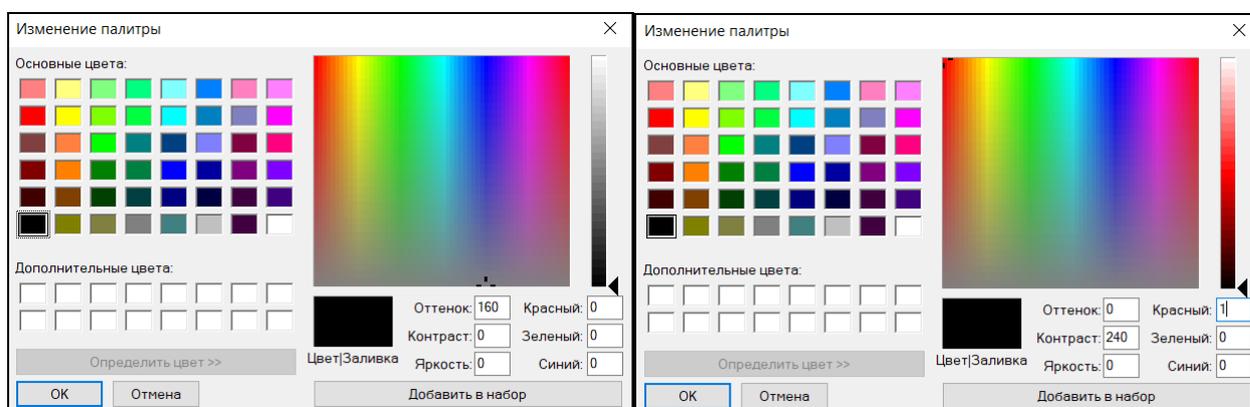


Рис. 13. Пример изменения параметров цвета

С помощью текста добавляем сообщение в контейнер. Получаем полностью однотонное изображение с скрытым сообщением (рис. 14).

Для дешифровки достаточно выбрать контрастный цвет и воспользоваться инструментом заливки в рандомной области изображения.

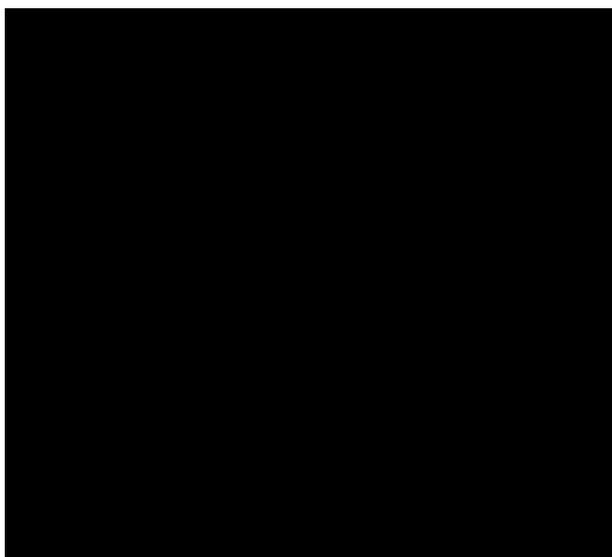


Рис. 14. Заполненный стегоконтейнер

Задание 2

Цифровой водяной знак (ЦВЗ) — технология, созданная для защиты авторских прав мультимедийных файлов. Обычно цифровые водяные знаки невидимы. Однако ЦВЗ могут быть видимыми на изображении или видео.

Задание: При помощи графического редактора Разработайте свой водяной знак и расположите его на изображении.

Рассмотрим пример выполнения задания при помощи Photoshop:

1. Создаем пустой слой в PhotoShop.
2. Выбираем инструмент «Текст» и пишем желаемый текст.
3. Выполните форматирование текста - измените цвет, размер и шрифт текста (рис. 15)



Рис. 15. Пример форматирования текста

4. Для выделения текста выберите слой с текстом, нажмите комбинацию клавиш CTRL+T.
5. Поверните текст (рис. 16).

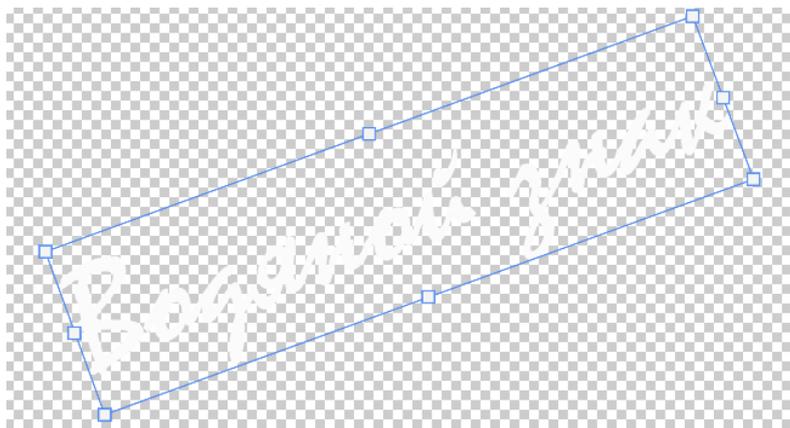


Рис. 16. Пример поворота текста

6. Настройте непрозрачность текста. Для этого выберите слой текста, и справа в верхнем углу выберите непрозрачность (рис. 17).

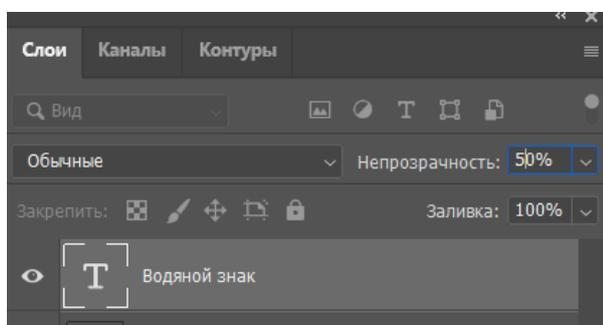


Рис. 17. Настройка непрозрачности

7. Сохраните полученное изображение в формате png.

Для расположения полученного водяного знака на изображении достаточно открыть его дополнительным слоем и настроить размещение.

Задание 3

Используя заказную палитру цветов и режим палитра цветов сделайте изображение визуально полностью черным. Оттенки черного должны быть различны для возможности восстановления изначального изображения.

Примечание! В заказной палитре необходимо изменить ее так чтобы все цвета имели один оттенок и яркость. Например, у первого цвета можем поставить следующие значения R: 0; G: 0; B: 255. Таким образом меняем значения у всех цветов так чтобы они были равны либо нулю, либо 255 и не повторялись. В режиме палитра цветов у каждого цвета значения меняем значение 255 на 2.

Задание 4

Дано полностью черное изображение используя автоконтраст раскройте скрытое изображение.

Раздел 3.

Раздел содержит ряд заданий, которые выполняются с использованием стеганографических приложений. Четыре первых задания исследовательского характера, пятое и шестое задание на сокрытие данных.

Задание 1

Произвести сопоставление различных стеганографических приложений и утилит.

Задание 2

Сопоставить алгоритмов, используемых в разных стеганографических приложениях.

Задание 3

С помощью стеганографических приложений изучить влияние объема скрываемого файла на степень искажения исходного графического контейнера.

Задание 4

С помощью стеганографических приложений изучить влияние объема скрываемого файла на степень искажения исходного аудио-контейнера.

Задание 5

Выполнить сокрытие различных данных в изображении при помощи стеганографического приложения.

Задание 6

Выполнить сокрытие различных данных в аудиофайле при помощи стеганографического приложения.

Раздел 4.

Четвертый раздел включает пять заданий в которых предлагается реализовать методы стеганографии на языке программирования. Для выполнения данных заданий необходимы знания по работе с файлами и строками, а

также умения реализовывать циклы. Первые три задания можно применить при изучении циклов.

Рассмотрим задания и их на языке Python.

Задание 1

Маша отправила Вите письмо с тайным посланием. Письмо представляет из себя текст. Каждое встречающееся в тексте число содержит в своем младшем байте ASCII-код некоторой буквы (большой или маленькой) английского алфавита.

Напишите программу, которая поможет Вите прочитать сообщение Маши.

Входные данные: Текстовая строка с сообщением.

Результат работы программы: Расшифрованное сообщение.

Пример:

Входные данные: Домашнее задание: Математика № 72, 105 стр.32. Русский № 86 стр. 105. Литература прочитать текст на стр. 99 – 116. Физика стр. 111 – 114.

Результат работы программы: Hi Victor

Решение:

Для решения данной задачи вначале программы задаем функцию для ввода Машиного письма с консоли, а также задаем три строковых переменных. В первой записаны все числа от 0 до 9. Вторая и третья пустые, одна для записи считаного числа, другая для записи расшифрованных символов сообщения.

Далее запускаем цикл, который считывает и проверяет символы сообщения. Если символ является числом, то записываем его в переменную k. Если все символы числа прочитаны, то переводим полученную цифру в символ, записываем его в переменную t и обнуляем переменную k.

В конце выводим расшифрованное сообщение на консоль.

На рис. 18 представлен пример реализации программы.

```

s = input("Введите текст с скрытым сообщением: ")
n = "1234567890"
k = ''
t = ''
for i in range(len(s)):
    if s[i] in n:
        k = k+s[i]
    if (k != '') and (s[i] not in n):
        t = t+chr(int(k))
        k = ''
print("Скрытое сообщение: ", t)

```

Рис. 18. Пример программы к Заданию 1

На рис. 19 представлен результат работы программы.

```

Введите текст с скрытым сообщением: Домашнее задание: Математика № 72, 105
стр.32. Русский № 86 стр. 105. Литература прочитать текст на стр. 99 - 116.
Физика стр. 111 - 114.
Скрытое сообщение: Hi Victor

```

Рис. 19. Результат работы программы

Задания 2 и 3 решаются подобным образом.

Задание 2

Маша отправила Вите письмо со скрытым сообщением. Известно, что оно было скрыто с помощью метода хвостовых пробелов.

Напишите программу, которая поможет Вите прочитать сообщение Маши.

Метод хвостовых пробелов

Каждый символ кодируется определенном двоичным кодом. Для определения этих кодов есть табличка ASCII, любой десятичный номер буквы в этой таблице можно представить в двоичном формате. Например, английская буква k имеет десятичный номер 107, а если перевести эту десятичную цифру в двоичное число в 8 битовом формате, то оно будет представлено вот таким образом 01101011.

После кодирования символов сообщения можно применить метод хвостовых пробелов. Он предполагает дописывание в конце каждой строки текстового файла одного пробела, в случае кодирования единичного бита стего-сообщения. Если нужно закодировать нулевой бит, пробел в конце строки не дописывается.

Входные данные:

В первой строке входных данных содержится единственное натуральное число N ($1 \leq N \leq 1000$) + количество строк в письме.

Далее вводятся N строк (Машино письмо).

Результат работы программы: Расшифрованное сообщение.

Пример:

Входные данные:

```
Не·верь,·не·верь·себе,·мечтатель·молодой,¶  
Как·язык,·бойся·вдохновенья...¶  
Оно·-·тяжелый·бред·души·твоей·больной¶  
Иль·пленной·мысли·раздраженье.¶  
В·нем·признака·небес·напрасно·не·ищи·-¶  
То·кровь·кипит,·то·сил·избыток!¶  
Скорее·жизнь·свою·в·заботах·истощи,¶  
Разлей·отравленный·напиток!¶  
Случится·ли·тебе·в·заветный,·чудный·миг¶  
Отрыть·в·душе·давно·безмолвной¶  
Еще·неведомый·и·девственный·родник,¶  
Простых·и·сладких·звучков·полный,-¶  
Не·вслушивайся·в·них,·не·предавайся·им.¶  
Набрось·на·них·покров·забвенья.¶  
Стихом·размеренным·и·словом·ледяным¶  
Не·передашь·ты·их·значенья.¶
```

Рис. 20. Пример входных данных к заданию 2

Результат работы программы: На.

Задание 3

Маша отправила Вите письмо со скрытым сообщением. Известно, что оно было скрыто с помощью метода хвостовых пробелов.

Напишите программу, которая поможет Вите прочитать сообщение Маши.

Метод двойных пробелов

Каждый символ кодируется определенном двоичным кодом. Для определения этих кодов есть табличка ASCII, любой десятичный номер буквы в этой таблице можно представить в двоичном формате. Например, английская буква *k* имеет десятичный номер 107, а если перевести эту десятичную цифру в двоичное число в 8 битовом формате, то оно будет представлено вот таким образом 01101011.

Форматирование текста количеством пробелов, отличным от единицы. Суть данного метода состоит в раздвижке строки путем увеличения пробелов

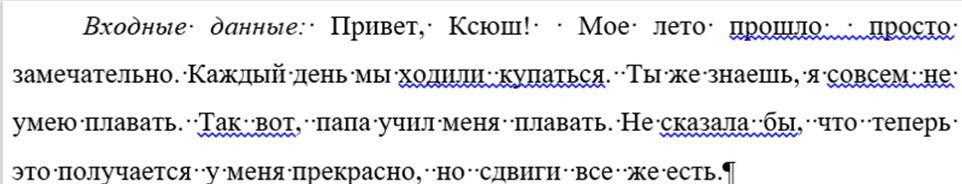
между словами, когда один пробел соответствует, например, биту 0, два пробела – биту 1.

Входные данные: Текстовая строка с сообщением.

Результат работы программы: Расшифрованное сообщение.

Пример:

Входные данные: Привет, Ксюш! Мое лето прошло просто замечательно. Каждый день мы ходили купаться. Ты же знаешь, я совсем не умею плавать. Так вот, папа учил меня плавать. Не сказала бы, что теперь это получается у меня прекрасно, но сдвиги все же есть.



Входные данные: Привет, Ксюш! Мое лето прошло просто замечательно. Каждый день мы ходили купаться. Ты же знаешь, я совсем не умею плавать. Так вот, папа учил меня плавать. Не сказала бы, что теперь это получается у меня прекрасно, но сдвиги все же есть.¶

Рис. 21. Пример входных данных к заданию 3

Результат работы программы: Harri.

Задания четыре и пять связаны с сокрытием данных в текстовых документах, их можно применять при изучении работы с файлами в языке программирования.

Задание 4

Напишите программу, которая будет скрывать тайное сообщение в текстовом документе с помощью метода хвостовых пробелов.

Каждый символ кодируется определенном двоичным кодом. Для определения этих кодов есть табличка ASCII, любой десятичный номер буквы в этой таблице можно представить в двоичном формате. Например, английская буква k имеет десятичный номер 107, а если перевести эту десятичную цифру в двоичное число в 8 битовом формате, то оно будет представлено вот таким образом 01101011.

После кодирования символов сообщения можно применить метод хвостовых пробелов. Он предполагает дописывание в конце каждой строки текстового файла одного пробела, в случае кодирования единичного бита стегосообщения. Если нужно закодировать нулевой бит, пробел в конце строки не дописывается.

Входные данные: Текст скрываемого сообщения

Результат работы программы: Файл с зашифрованным сообщением.

Решение:

Для решения данной задачи вначале программы создаем две строковых переменных eng и rus содержащих буквы, пошившиеся одинаково в английском и русском языках соответственно. Задаем функцию для ввода сообщения которое необходимо скрыть, открываем два файла с текстом, в котором будет скрываться сообщение и пустой (новый) для записи зашифрованных данных (рис. 22).

```
rus = 'АВЕКМОРСТХаеорсх'  
eng = 'АВЕКМОРСТХаеорсх'  
  
to_encode = input('Введите тайное сообщение: ')  
  
text = open('text.txt', 'r', encoding='utf-8')  
encoded = open('encoded.txt', 'w')
```

Рис. 22. Вводные данные программы

Далее запускаем цикл который читает данные файла с текстом и побуквенно кодирует сообщение и записывает полученные данные в новый файл. Цикл прерывается если заканчиваются символы в файле с текстом или сообщении (рис. 23).

```
n=0  
k=0  
bits=8  
while True:  
    symbol_text = text.read(1)  
    if not symbol_text:  
        break  
  
    if symbol_text in eng:  
  
        if bits == 8:  
            bits = 0  
            n += 1  
  
            if n == len(to_encode):  
                encoded.write(symbol_text)  
                break  
  
            #считываем код символа  
            k=ord(to_encode[n])  
  
            b=''  
  
            #переводим считываемый код в двоичное число  
            while k>0:  
                b=str(k%2)+b  
                k =k//2  
            #переводим полученное двоичное число в 8-ми битовую систему  
            while len(b)<8:  
                b='0'+b  
  
            if int(b[bits]) == 1:  
                symbol_text = rus[eng.index(symbol_text)]  
                bits += 1
```

Рис. 23. Пример реализации функции кодирования

Дочитываем данные из текста и записываем в файл с зашифрованными данными. Закрываем все документы (рис. 24).

```
encoded.write(text.read())  
  
text.close()  
encoded.close()
```

Рис. 24. Заключительная часть программы

При запуске программы на консоли всплывает запрос на ввод сообщения которое вам необходимо скрыть. После ввода сообщения создается новый документ `encoded.txt`, визуально не отличающимся от `text.txt`. Этот файл содержит в себе скрытое сообщение.

Задание 5

Напишите программу, которая будет скрывать тайное сообщение в текстовом документе с помощью изменения количества пробелов.

Каждый символ кодируется определенном двоичным кодом. Для определения этих кодов есть табличка ASCII, любой десятичный номер буквы в этой таблице можно представить в двоичном формате. Например, английская буква `k` имеет десятичный номер `107`, а если перевести эту десятичную цифру в двоичное число в 8 битовом формате, то оно будет представлено вот таким образом `01101011`.

Форматирование текста количеством пробелов, отличным от единицы. Суть данного метода состоит в раздвижке строки путем увеличения пробелов между словами, когда один пробел соответствует, например, биту `0`, два пробела – биту `1`.

Входные данные: Текст скрываемого сообщения

Результат работы программы: Файл с зашифрованным сообщением.

Последнее задание связано с сокрытием информации в изображениях.

Задание 6

Разработать программу, добавляющую ASCII-код одного знака текста к RGB-кодам пикселя и сохраняющую файл в графическом формате с последующей возможностью извлечения скрытой информации.

Раздел 5.

Раздел содержит пять олимпиадных заданий, два из которых подразумевают написание программы, три – нахождение скрытых сообщений в различных форматах данных.

Рассмотрим примеры заданий и их решения.

Задание 2

Алиса решила отправить Бобу сообщение. Но сейчас идет урок информатики, и просто так передать Бобу записку с текстом нельзя. Поэтому Алиса решила скрыть свое сообщение в массиве целых положительных чисел и передать Бобу этот массив в надежде, что Боб сможет извлечь из этого массива ее сообщение. Каждое переданное Алисой число содержит в своем младшем байте ASCII+код некоторой буквы (большой или маленькой) английского алфавита.

Напишите программу, которая поможет Бобу прочитать сообщение Алисы.

Формат входных данных

В первой строке входных данных содержится единственное натуральное число N ($1 \leq N \leq 1000$) + количество чисел в переданном массиве.

Во второй строке входных данных содержатся N положительных целых чисел A_i , каждое из которых не превышает 10^9 и содержит в своем младшем байте ASCII+код некоторой буквы английского алфавита.

Формат результата

Выведите единственную строку, состоящую ровно из N букв, скрытых в переданном Алисой массиве.

Примеры

Входные данные

```
3
97 98 99
```

Результат работы

```
abc
```

Входные данные

5
72 101 108 108 111

Результат работы

Hello

Входные данные

14
72 105 66 111 98 72 111 119 65 114 101 89 111 117

Результат работы

HiBobHowAreYou

Решение:

В начале программы задаем две функции читающие данные с консоли. Одна для ввода количества чисел, вторая для чтения зашифрованного сообщения для ввода чисел через пробел используется метод `split`. Далее запускается цикл переводящий полученные значения в символы и выводящий их на консоль (рис. 25).

```
# ввод количества символов
n = int(input())
# вод сообщения
s = input().split()

#расшифровка сообщения
for i in range(n):
    print(chr(int(s[i])),end='')
```

Рис. 25. Пример программы, реализующий расшифровку сообщения

На рис. 26 представлены примеры результатов работы программы.

```
3
97 98 99
abc

5
72 101 108 108 111
Hello

14
72 105 66 111 98 72 111 119 65 114 101 89 111 117
HiBobHowAreYou
```

Рис. 26. Результат работы программы

Задание 3

Аналитику удалось обнаружить папку с графическими изображениями (рис. 27), в которой скрыто осмысленное кодовое слово. Помогите определить кодовое слово, если известно, что для его сокрытия содержимое файлов не менялось.

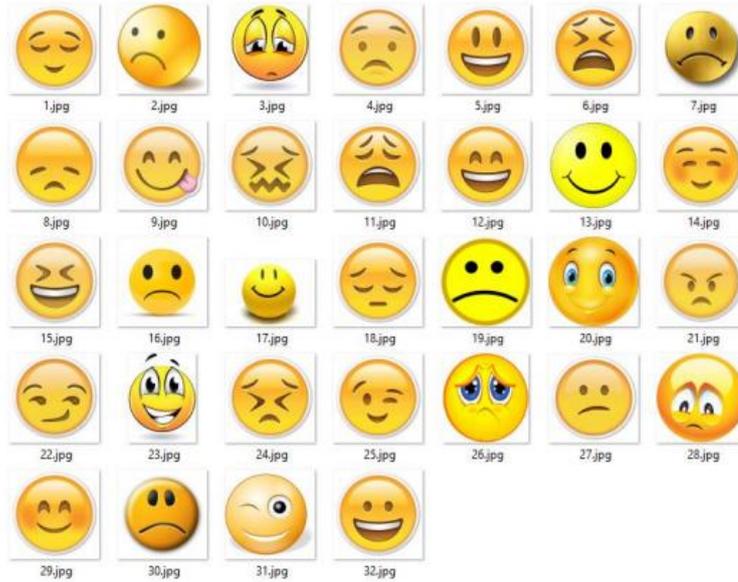


Рис. 27. Прилагаемые изображения

Решение:

Представленные изображения расположены в определенном порядке можно предположить, что они кодируют значения битов. Улыбающиеся смайлик кодирует 0, а грустный 1.

Учитывая это получаем следующие значения: 01110111 01100011 01101001 01110100.

Переводим полученные значения в десятичные и при помощи таблицы кодировки ASCII получаем скрытое сообщение.

Ответ: wсit.

В модуле «Проекты» приводятся примеры тем для проектов по стеганографии и их краткая аннотация. Данный модуль содержит три блока: стеганография в пользовательских приложениях, стеганография в специализированных приложениях, программирование стеганографических методов.

Стеганография в пользовательских приложениях:

1. Реализация некомпьютерных методов стеганографии в текстовом редакторе.

В теоретической части проекта рассматриваются некомпьютерные методы стеганографии. В практической части анализируются возможности современных текстовых редакторов. Выполняется реализация некомпьютерных методов стеганографии с использованием текстовых редакторов.

2. Стеганография раньше и сейчас.

В теоретической части рассматриваются основные понятия стеганографии, приводятся некомпьютерные и простейшие компьютерные методы стеганографии. В практической части разрабатывается обучающий видеоролик «Тайны сокрытия информации». Рассказывающий о важности стеганографии в современном мире, показывает на примерах как можно скрыть информации в при помощи текстовых и графических редакторов.

3. Сокрытие данных в изображениях с помощью Photoshop.

Рассматриваются методы сокрытия данных в изображения. Выполняется их реализация с помощью программы Photoshop.

4. Использование цифровых водяных знаков для защиты авторских прав.

Рассматриваются основные понятия и способы встраивания ЦВЗ. Приводятся примеры встраивания ЦВЗ при помощи пользовательских приложений. Анализируются возможности современных графических приложений для встраивания ЦВЗ.

5. Стеганография в формате GIF.

В проекте рассматриваются способы стеганографии применимые для формата GIF. Разрабатывается и приводится реализация метода скрывания информации в графических редакторах.

Стеганография в специализированных приложениях:

1. Влияние стегосообщения на контейнер.

В проекте рассматриваются и сопоставляются стеганографические приложения, позволяющие скрыть данные в изображениях. Анализируется влия-

ние размера скрываемой информации на контейнер. Даются рекомендации по выбору контейнера на основе проученных результатов.

2. Сопоставление специализированных стеганографических приложений.

В проекте рассматриваются основные стеганографические приложения. Проводиться сопоставительный анализ приложений. Даются рекомендации по выбору приложения.

Программирование стеганографических методов:

1. Соккрытие текстовой информация в изображении с помощью LSB методов.

В проекте рассматриваются цифровые методы стеганографии изображений. Разрабатывается программа реализующая метод LSB. Данная программа включает в себя функции кодирования и декодирования сообщения, а также позволяет выбрать изображение-контейнер и скрываемую информацию.

2. Соккрытие данных в аудиофайлах.

В проекте рассматриваются методы сокращения данных в звуковых файлах. Разрабатывается программа, реализующая стеганографический метод позволяющий скрыть изображение в аудиофайле. Данная программа включает в себя функции кодирования и декодирования сообщения, а также позволяет выбрать аудиофайл-контейнер и скрываемые данные.

3. Соккрытие данных в текстовом редакторе.

В проекте рассматриваются методы сокращения данных в тексте. Разрабатывается программа, реализующая стеганографический методы, позволяющие скрыть сообщение в текстовом файле. Данная программа включает в себя функции кодирования и декодирования сообщения, позволяет выбрать метод сокращения, а также аудиофайл-контейнер и скрываемую информацию.

4. Соккрытие графической информация в изображении с помощью LSB методов.

В проекте рассматриваются цифровые методы стеганографии изображений. Разрабатывается программа реализующая метод LSB. Данная программа включает в себя функции кодирования и декодирования сообщения, а также позволяет выбрать изображение-контейнер и скрываемые данные.

5. Соккрытие данных в видеофайлах.

В проекте рассматриваются структура видеофайла, а также цифровые методы стеганографии изображений. Разрабатывается программа реализующая метод LSB для видеофайла. Данная программа включает в себя функции кодирования и декодирования сообщения, а также позволяет выбрать изображение-контейнер и скрываемые данные.

Представленный в модулях «Задачи по реализации методов стеганографии» и «Проекты» перечень задач и проектов следует рассматривать как начальный – он легко может быть дополнен преподавателем, ведущим обучение, с учетом необходимых для его курса акцентов. Представляется полезным также участие в разработке и решении подобных задач самих учащихся.

Таким образом, ООР «Стеганография» включает образцы заданий, которые могут быть использованы преподавателем при изучении различных разделов информатики и информационных технологий даже без последовательного изложения алгоритмов и методов стеганографии.

2.3. Организация опытно-поисковой работы и ее результаты

Целью опытно-поисковой работы исследования является проверка исходной гипотезы: Разработанный ресурс «Стеганография» является открытым образовательным ресурсом и может быть использован для создания курсов по информатике и самостоятельного обучения.

Для достижения поставленной цели была организована апробация – методом экспертных оценок. В исследовании участвовали преподаватели Института математики, физики и информатики, а также действующие учителя информатики.

Анкетирование проводилось с использованием GoogleForme (рис.28). Для оценки ресурса было составлено восемь вопросов:

1. Необходимость изучения методов стеганографии в курсах информатики различного уровня.

2. Достаточность материалов, представленных в данном ресурсе, для освоения методов стеганографии.
3. Качество разработанных материалов.
4. Обоснованность использования идеологии открытого образовательного ресурса для обучения стеганографии (на основе открытых лицензий).
5. Возможность использования отдельных ресурсов и задач в курсах информатики и ИТ различного уровня.
6. Возможность использования ресурса для самостоятельного обучения.
7. Актуальность предложенных тем проектов учащихся по теме стеганография.
8. Пожелания/замечания по представленному ресурсу.

Экспертная оценка открытого образовательного ресурса "Стеганография"

Уважаемые коллеги! Прошу ответить на ряд вопросов, касающихся разработанного мною открытого образовательного ресурса «Стеганография».

foxdariya69@gmail.com Сменить аккаунт

Совместный доступ отсутствует

*Обязательный вопрос

Необходимость изучения методов стеганографии в курсах информатики различного уровня. *

1 2 3 4 5 6 7 8 9 10

○ ○ ○ ○ ○ ○ ○ ○ ○ ○

Достаточность материалов, представленных в данном ресурсе, для освоения методов стеганографии. *

1 2 3 4 5 6 7 8 9 10

○ ○ ○ ○ ○ ○ ○ ○ ○ ○

Качество разработанных материалов. *

Рис. 28. Анкета экспертов в GoogleForme

Первые семь вопросов оцениваются по десятибалльной шкале, восьмой предусматривает краткий ответ в свободной форме.

В результате опроса действующих учителей информатики были получены следующие результаты (табл. 6).

ОТВЕТЫ ЭКСПЕРТОВ

	Вопрос 1	Вопрос 2	Вопрос 3	Вопрос 4	Вопрос 5	Вопрос 6	Вопрос 7
Эксперт 1	6	10	9	9	8	5	8
Эксперт 2	9	10	10	9	10	10	10
Эксперт 3	9	10	10	10	10	10	10
Эксперт 4	10	10	10	10	10	10	10
Эксперт 5	4	9	9	10	4	9	8
Эксперт 6	9	10	10	10	10	10	10
Эксперт 7	10	9	9	8	9	9	8
Эксперт 8	10	10	8	10	10	10	8
Эксперт 9	8	7	7	7	8	9	7
Эксперт 10	7	8	4	8	8	8	8
Ср.знач.	8,2	9,3	8,6	9,1	8,7	9	8,7

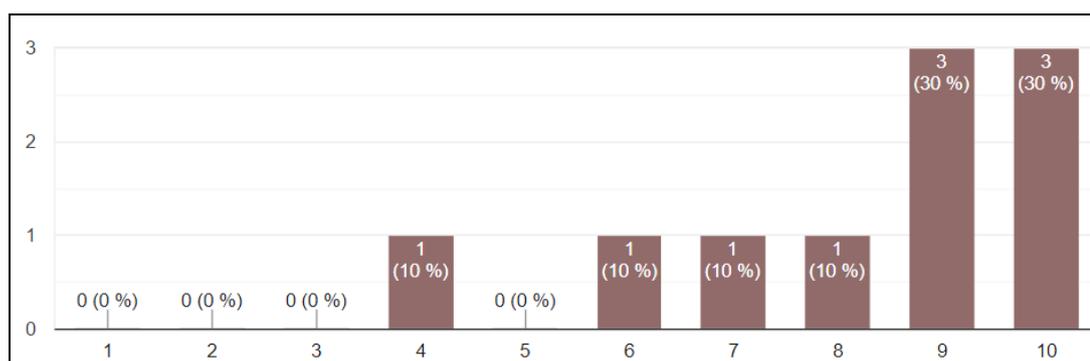


Рис. 29. Диаграмма, отражающая оценку экспертов необходимости изучения методов стеганографии в курсах информатики различного уровня

На основании полученной диаграммы к первому вопросу (рис. 29) можно заметить, что некоторые учителя не считают возможным обучение методам стеганографии в курсе информатики. Однако большинство экспертов отмечают важность изучения данной темы. На этаже указывает высокая средняя оценка – 8,2.

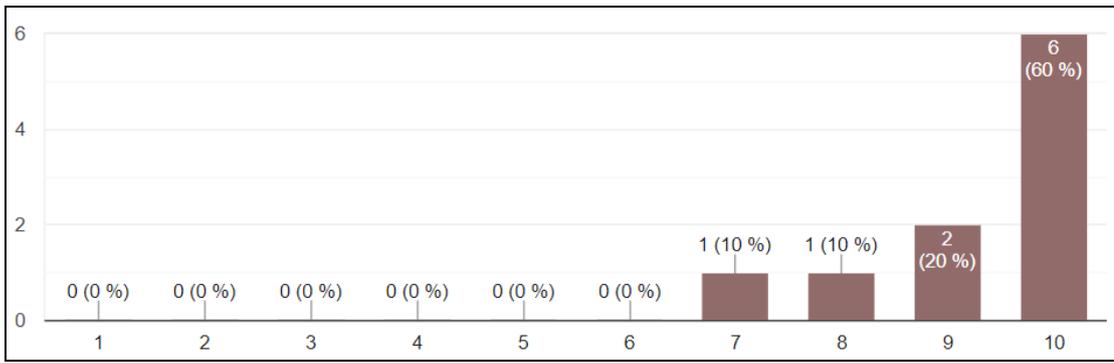


Рис. 30. Диаграмма, отражающая оценку экспертами достаточности материалов, представленных в данном ресурсе, для освоения методов стеганографии

Большинство экспертов отметило достаточность материалов для освоения методов стеганографии (рис. 30).

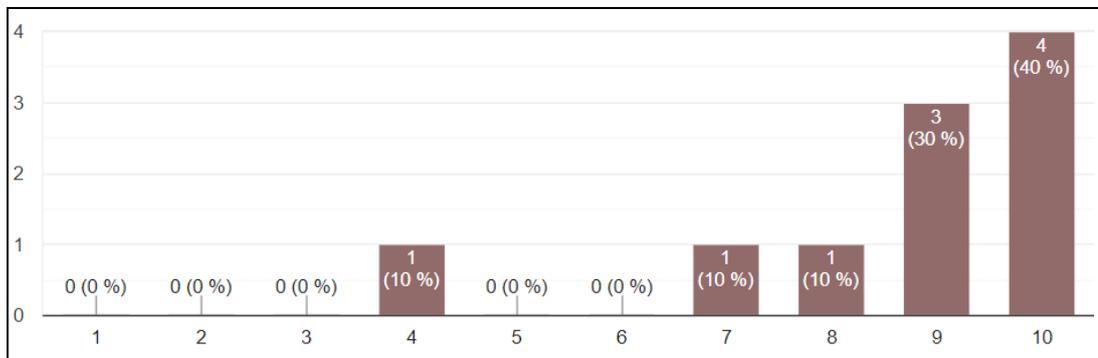


Рис. 31. Диаграмма, отражающая оценку экспертами качество разработанных материалов

На основании диаграммы, представленной на рис. 31, можно сделать вывод, что материалы, представленные в ресурсе, разработаны качественно.

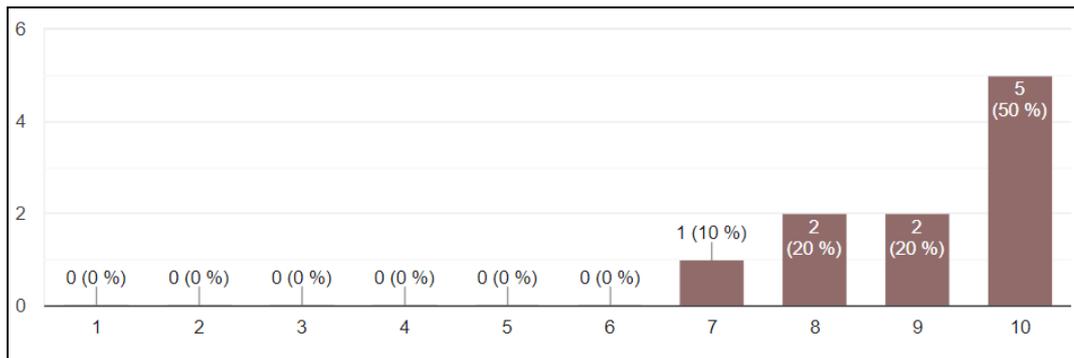


Рис. 32. Диаграмма, отражающая оценку экспертами обоснованности использования идеологии открытого образовательного ресурса для обучения стеганографии (на основе открытых лицензий).

Результаты опроса (рис.32) по четвертому вопросу позволяют сделать вывод, что разработанный ресурс является открытым образовательным ресурсом.

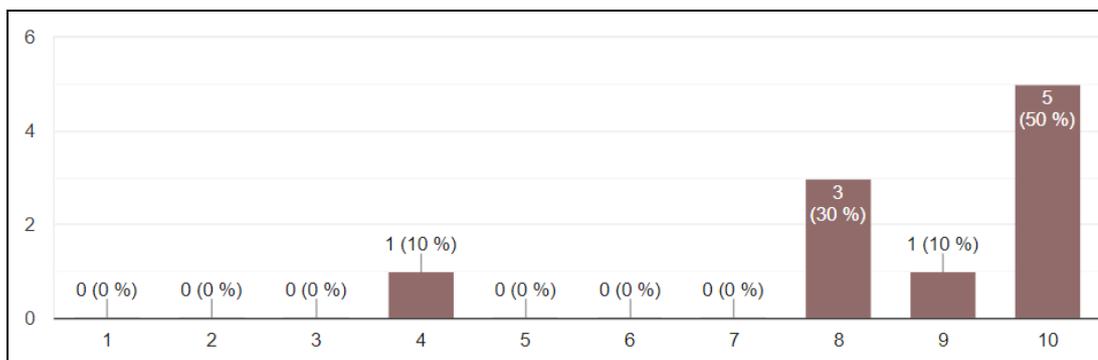


Рис. 33. Диаграмма, отражающая оценку экспертами возможности использования отдельных ресурсов и задач в курсах информатики и ИТ различного уровня

На основании полученной той диаграммы к пятому вопросу (рис. 33) можно заметить, что некоторые учителя считают маловероятным использование отдельных ресурсов и задач в курсах информатики и ИТ различного уровня. Однако большое количество высоких оценок экспертов в пятом вопросе подчеркивают обратное.

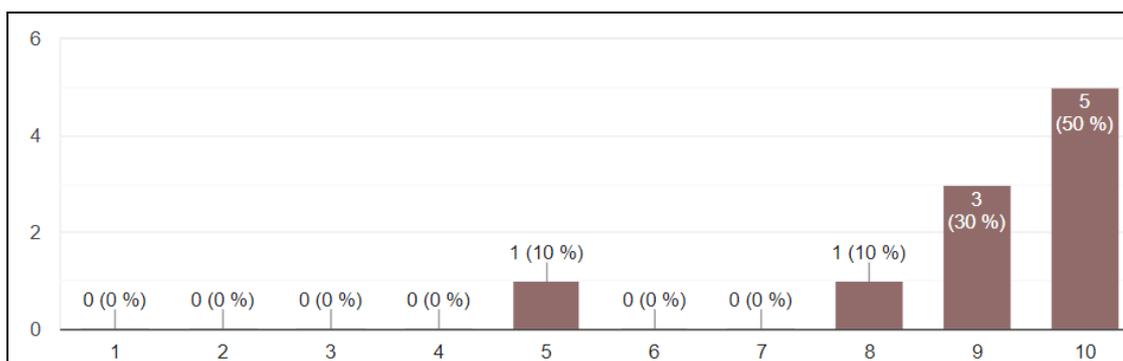


Рис. 34. Диаграмма, отражающая оценку экспертами возможности использования ресурса для самостоятельного обучения

Результат опроса (рис. 34) показывает возможность использования ресурса для самостоятельного обучения.

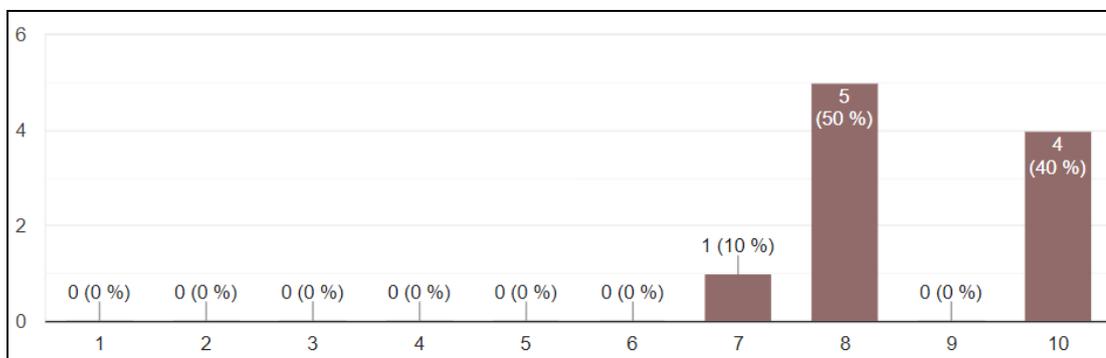


Рис. 35. Диаграмма, отражающая оценку экспертами актуальности предложенных тем проектов учащихся по теме стеганография

Большинство экспертов отмечают актуальность предложенных тем проектов учащихся по теме стеганография (рис. 35).

В рамках последнего вопроса было получено следующие пожелания:

- добавить больше задач на программирование;
- добавить формулировки к некоторым заданиям;
- добавить в лабораторных работах цели (задачи).

Таким образом, результаты опытно-поисковой работы позволяют сделать вывод, что разработанный ресурс «Стеганография» является открытым образовательным ресурсом и может быть использован для создания курсов по информатике и самостоятельного обучения. После отдельных незначительных доработок данный ресурс может быть рекомендован к использованию.

Заключение

Сопоставление результатов работы с поставленными задачами позволяет сделать следующие выводы:

1. На основе произведенного анализа библиографических данных, посвященных теме «Стеганография», обоснована необходимость изучения стеганографии в курсах информатики различного уровня для иллюстрации современных средств защиты информации.

2. На основе произведенного анализа технологии цифровой стеганографии было выделены подходы к решению задач цифровой стеганографии: инструментальный, программный и с помощью приложений общего назначения.

3. Для разработки педагогической модели облачного информационного открытого образовательного ресурса сформулированы и обоснованы следующие принципы построения ресурса: модульность, расширяемость контента, облачное размещение, полнота охвата по содержанию и методам, гибкость использования. Было выделено шесть модулей: введение в стеганографию, стеганография в специализированных приложениях, стеганография в пользовательских приложениях, программирование стеганографических методов, задачи по реализации методов стеганографии, стеганографические проекты. Были предложены варианты применения разработанного ресурса.

4. На основе разработанной структуры и общего содержания был разработан открытый образовательный ресурс по теме «Стеганография» с открытой лицензией использования Creative Commons. Разработаны комплекты учебных заданий, которые могут применяться в курсе информатики, а также темы проектов по стеганографии.

5. Проведенное опытно-поисковое исследование доказало, что разработанный ресурс «Стеганография» является открытым образовательным ресурсом и может быть использован для создания курсов по информатике и самостоятельного обучения.

Таким образом, следует считать, что задачи исследования полностью выполнены, цель достигнута. Работу можно считать завершенной.

Источники информации

1. Абазина, Е. С. Цифровая стенография: состояние и перспективы / Е. С. Абазина, А. А. Ерунов // Системы управления, связи и безопасности. – 2016. – №2. – С.182-200.
2. Аль-Аммори, А. Методы и средства защиты информации / А. Аль-Аммори // The Scientific Heritage. – 2020. – №51. – С. 32-42.
3. Андроник К. Особенности использования и перспективы компьютерной стеганографии / К. Андроник, В. Власов // Securitatea informațională. – 2010. – С.71-74.
4. Анисимов, В. В. Криптографические методы защиты информации. Стеганография / В. В. Анисимов : [сайт]. – URL: <https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema19> (дата обращения: 13.11.2022).
5. Батаева, И. П. Защита информации и информационная безопасность / И. П. Батаева // Труды Международного симпозиума «Надежность и качество». – 2012. – Т.1. – С.116-118.
6. Белкина, Т. А. Аналитический обзор применения сетевой стеганографии для решения задач информационной безопасности / Т. А. Белкина // Молодой ученый. – 2018. – № 11 (197). – С. 36-44.
7. Блинова, Е. А. Применение нескольких стеганографических методов для осаднения скрытых данных в электронных текстовых документах / Е. А. Блинова, А. А. Суцены // Системный анализ и прикладная информатика. – 2019. – № 2. – С. 32-38.
8. Буйлова, Л. Н. О методических аспектах разработки модульных дополнительных общеразвивающих программ / Л. Н. Буйлова // Про_ДОТ. – 2022. – №3(39). – С. 5-18.
9. Грибунин, В. Г. Цифровая стеганография./ В. Г. Грибунин, И. Н. Оков, И. В. Туринцев // М.: Солон-Пресс, 2009. – 272 с.
10. Днепровская, Н. В. Открытые образовательные ресурсы: современные перспективы / Н. В. Днепровская, И. В. Шевцова // Высшее образование в

- России. – 2019. – Т. 28. – № 8-9. – С. 110-118. – DOI 10.31992/0869-3617-2019-28-8-9-110-118.
11. Конахович, Г. Ф. Компьютерная стеганография. Теория и практика. / Г. Ф. Конахович, А. Ю. Пузыренко // Киев : МК-Пресс, 2006 .– 288 с.
 12. Краева, Е. В. Актуальность стеганографии и ее практическое применение / Е. В. Краева, Т. М. Татарникова, С. А. Веревкин [и др.] // Информационные технологии и системы: управление, экономика, транспорт, право. – 2019. – № 3(35). – С. 105-109.
 13. Марков, А. С. Основы криптографии: подготовка к CISSP / А. С. Марков, В. Л. Цирлов // Вопросы кибербезопасности. – 2015. – № 1(9). – С. 65-73.
 14. Обиденко, А. В. Обоснование необходимости обеспечения информационной безопасности предприятия в эпоху цифровизации / А. В. Обиденко, А. В. Шабурова // Интерэкспо Гео-Сибирь. – 2021. – Т. 6. – С. 235-239.
 15. Олимпиаева, Н. И. Методика текстовой стеганографии с использованием графического контейнера на основе гаммирования / Н. И. Олимпиаева, В. М. Довгаль, Л. С. Крыжевич // Auditorium. – 2018. – № 2(18). – С. 54-61.
 16. Поляков, К. Ю. Информатика. Углубленный уровень : Учебник для 10 класса. В двух частях. Часть 2/ К. Ю. Поляков, Е. А. Еремин. – Москва : ООО "Издательство "БИНОМ. Лаборатория знаний", 2013. – 304 с.
 17. Практическая стеганография: [сайт]. – URL: <https://habr.com/ru/company/crosstech/blog/440824/> (дата обращения: 13.11.2022).
 18. Слипенчук, П. В. Перспективы и практическое применение стеганографии в помехоустойчивых кодах / П. В. Слипенчук // Безопасность информационных технологий. – 2014. – Т. 21. – № 3. – С. 123-129.
 19. Стариченко Б.Е. Теоретические основы информатики / Б. Е. Стариченко // Учебник для вузов. – 3-е изд. перераб. и доп. – М.: Горячая линия – Телеком, 2016. – 400 с.

20. Стариченко, Б. Е. Методы цифровой стеганографии в курсе «теоретические основы информатики» / Б. Е. Стариченко, Л. В. Сардак // Информатизация образования и методика электронного обучения: цифровые технологии в образовании : Материалы V Международной научной конференции. В 2-х частях, Красноярск, 21–24 сентября 2021 года / Под общей редакцией М.В. Носкова. – Красноярск: Сибирский федеральный университет, 2021. – С. 476-481.
21. Стеганография в XXI веке. Цели. Практическое применение. Актуальность: [сайт]. – URL: <https://habr.com/ru/post/253045/> (дата обращения: 13.11.2022).
22. Федеральный государственный образовательный стандарт основного общего образования Утвержден приказом Министерства просвещения российской федерации от 31.05.2021. № 287. 129 с.
23. Хилен, Я. Появление открытых образовательных ресурсов (англ.). / Я. Хилен // Париж, Франция: Организация экономического сотрудничества и развития. – 2007. – С. 30.
24. Частикова, В. А. Методика распознавания скрытой информации в изображениях на основе алгоритмов стеганографии / В. А. Частикова, Т. О. Аббасов, С. С. Аббасова // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2020. – № 3(266). – С. 40-45.
25. Шутько Н. П. Алгоритмы реализации методов текстовой стеганографии на основе модификации пространственно-геометрических и цветовых параметров текста / Труды БГТУ. – 2016. – №6. – С.160-165.
26. Шутько, Н. П. Алгоритмы реализации методов текстовой стеганографии на основе модификации пространственно-геометрических и цветовых параметров текста / Н. П. Шутько // Труды БГТУ. №6. Физико-математические науки и информатика. – 2016. – № 6(188). – С. 160-165.
27. ЮНЕСКО цифровая библиотека: Форум по влиянию открытых учебных курсов на высшее образование в развивающихся странах: итоговый от-

- чет. – Париж – 2002. – 30 с. – URL:
<http://unesdoc.unesco.org/images/0012/001285/128515e.pdf>. (дата обращения: 13.11.2022)
28. CoreApp: [сайт]. – URL: <https://coreapp.ai/> (дата обращения: 19.03.2023).
29. Creative Commons: [сайт]. – URL: <https://creativecommons.org/> (дата обращения: 24.04.2023).
30. DarkCryptTC : [сайт]. – URL:
<http://www.cdmail.ru/security/passwords/darkcrypttc-shifrovanie-v-totalcommander.htm> (дата обращения: 03.01.2023).
31. DeepSound // SoftPedia : [сайт]. – URL:
<https://www.softpedia.com/get/Security/Encrypting/DeepSound.shtml> (дата обращения: 03.01.2023).
32. Google Класс : [сайт]. – URL: <https://classroom.google.com/u/0/h> (дата обращения: 19.03.2023).
33. ImageSpyer G2 // FreeSoft : [сайт]. – URL:
https://freesoft.ru/windows/imagespyer_g2 (дата обращения: 03.01.2023).
34. Moodle : [сайт]. – URL: <https://moodle.org/?lang=ru> (дата обращения: 19.03.2023).
35. OpenStego // SourceForge : [сайт]. – URL:
<https://sourceforge.net/projects/openstego/files/> (дата обращения: 03.01.2023).
36. RedJPEG XT // FreeSoft : [сайт]. – URL:
https://freesoft.ru/windows/redjpeg_xt (дата обращения: 03.01.2023).
37. Steganos Privacy Suite // SoftPortal : [сайт]. – URL:
<https://www.softportal.com/software-31023-steganos-privacy-suite.html> (дата обращения: 03.01.2023).
38. StegoStick // SourceForge : [сайт]. – URL:
<https://sourceforge.net/projects/stegostick/> (дата обращения: 03.01.2023).