Приложение 3

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ГОРОДА МОСКВЫ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГОРОДА МОСКВЫ

«КОЛЛЕДЖ СВЯЗИ №54»

ИМЕНИ П.М. ВОСТРУХИНА

Специальность

КУРСОВАЯ РАБОТА

по МДК.02.01. «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты» и

МДК.02.02. «Криптографическая защита информации»

Студента _____

(фамилия, имя, отчество)

Группы _____

на тему: «_____»

Руководитель: преподаватель спецдисциплин,

_____

(должность ФИО)

Руководитель: преподаватель спецдисциплин,

_____

(должность ФИО)

Оценка _____ /_____/_____/

(Подпись преподавателя) (Подпись преподавателя)

Дата «_____» _____2023 г.

Москва 2023

Приложение 4

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ГОРОДА МОСКВЫ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГОРОДА МОСКВЫ

«КОЛЛЕДЖ СВЯЗИ №54»

ИМЕНИ П.М. ВОСТРУХИНА

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студенту:_____

(фамилия, имя, отчество полностью)

I. Тема курсовой работы:

_____

_____

_____

II. Срок сдачи студентом законченной работы:

_____

III. Исходные данные:

1. _____
2. _____

IV. Перечень подлежащих разработке вопросов:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____

V. Перечень графического /иллюстрационного материала:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

VI. Дата выдачи задания «___»_____2023 г.

Руководитель _____ _____

(ФИО) (подпись)

Руководитель _____ _____

(ФИО) (подпись)

Задание принял к исполнению _____ _____

(ФИО) (подпись)

«____»_____2023 г.

Приложение 5

«УТВЕРЖДАЮ»
_Председатель ПЦК
_____ Е. Е. Сверчков
«_____» _____ 20__г.

ПЛАН-ГРАФИК

подготовки и выполнения курсовой работы

студента ____ курса группы _____ отделения ____

_____

тему _____

№ п/г	Выполняемые работы и мероприятия	Срок выполнения	Отметка руководителя о завершении этапа **(число и подпись)**
1	Введение	17.04.2023	
2	Глава 1	27.04.2023	
3	Глава 2	06.05.2023	
4	Заключение и литература	11.05.2023	
5	Разработка тезисов для защиты и презентации	15.05.2023	
6	Защита курсовой работы	20.05.2023	

Подпись руководителя _____

Подпись руководителя _____

С графиком выполнения работы ознакомлен:

Подпись студента _____

Дата «_____»_____ 20___г.

Оглавление

Введение

Сокрытие информации в графических файлах - это техника, которая позволяет скрыть информацию в изображениях, не нарушая их внешний вид. Эта техника является одним из наиболее распространенных методов стеганографии, которая используется для передачи скрытых сообщений без вызова подозрений у посторонних наблюдателей. Стеганография имеет множество применений, включая конфиденциальную передачу данных, защиту информации, цифровую подпись, а также в области криминалистики для обнаружения скрытой информации в изображениях. В данной курсовой работе мы рассмотрим основные методы сокрытия информации в графических файлах, их преимущества и недостатки, а также возможности для их применения в реальных ситуациях.

Задачей криптографии является скрытие информации, содержащейся в сообщении, за счет его шифрования, а стеганография (пер. с греч, "тайнопись") - это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи. Главная задача сделать так, чтобы человек не подозревал, что внутри передаваемой информации, внешне не представляющей абсолютно никакой ценности, содержится секретная информация. Тем самым стеганография позволяет передавать важную информацию через открытые каналы, скрывая сам факт её передачи. В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает само его существование. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

Актуальность темы обусловлена тем, что большинство информации при передаче по открытым каналам передачи информации может быть перехвачена, а через методы стеганографии текст будет находится в неком контейнере, которое если и перехватят, то будут трудности с ее раскрытием.

Целью данной курсовой работы является исследование основных способов сокрытия информации, и в частности методов компьютерной стеганографии.

Задачи работы:

– Изучение теоретической информации по сокрытию информации в графических файлах

– Изучение основных методов и способов сокрытия информации в графических файлах

– Описать модель и принцип работы стеганосистем

– Произвести обзор некоторых методов компьютерной стеганографии

Глава 1. Анализ основ сокрытия информации в графических файлах.

1.1. Нормативно-правые акты в области криптографической защиты.

Положение «О лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных (истем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»

1. Настоящее Положение определяет порядок лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств,

осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), осуществляемой юридическими лицами и индивидуальными предпринимателями (далее - лицензируемая деятельность).

2. К шифровальным (криптографическим) средствам (средствам криптографической защиты информации), включая документацию на эти средства, относятся:

- средства шифрования - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче;

- средства имитозащиты - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации;

- средства электронной подписи;

- средства кодирования - средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций;

- средства изготовления ключевых документов - аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств;

- ключевые документы - электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах;

- аппаратные шифровальные (криптографические) средства - устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин;

- программные шифровальные (криптографические) средства - программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств;

- программно-аппаратные шифровальные (криптографические) средства - устройства и их компоненты (за исключением информационных систем и телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для электронных вычислительных машин, предназначенных для осуществления этих преобразований информации или их части.

На практике методы стеганографии применяются для идентификации, защиты авторских прав и сокрытия передаваемых сообщений.

Хранение изображений в цифровом формате упрощает их хранение и распространение, но также увеличивает риск нарушения авторских прав, несанкционированного изменения и распространения. В целях защиты интеллектуальной собственности и определения изменений, разрабатываются и применяются цифровые водяные знаки. К таким стеганографическим методикам предъявляются особые требования:

- Качество исходного изображения не должно быть серьёзно затронуто, скрытые данные должны быть минимально заметны.

- Скрытые данные должны сохраняться в разных форматах, то есть содержаться не только в заголовке, а во всем теле изображения.

- Скрытые данные должны быть устойчивы к намеренным попыткам удаления.

- Необходимо наличие избыточного кода для коррекции ошибок, так как деградация данных при передаче/модификации неизбежна.

1.2. Описание стеганографии

Сокрытие информации в графических файлах - это процесс внедрения дополнительных данных в графический файл, не влияющих на его внешний вид, с целью передачи скрытого сообщения без вызова подозрений у третьих лиц.

Основными методами сокрытия информации в графических файлах являются:

- Методы замены пикселей: данный метод основывается на замене значений пикселей графического файла на значения, которые кодируют информацию. Так, например, можно заменить наименее значимые биты RGB компонент каждого пикселя, чтобы внедрить скрытое сообщение.

- Методы изменения структуры: в этом случае используется изменение структуры графического файла, путем перемещения блоков пикселей или изменения порядка следования пикселей. Этот метод может быть более

надежным, чем метод замены пикселей, но при этом может привести к незначительным изменениям внешнего вида графического файла.

- Методы изменения цветовой палитры: цветовая палитра графического файла может быть изменена таким образом, чтобы включить в нее дополнительные цвета, которые кодируют информацию.

- Методы изменения размера: изменение размера графического файла может быть использовано для внедрения скрытого сообщения, путем внедрения дополнительной информации в пустые пространства.

- Методы преобразования: применение математических преобразований, таких как дискретное преобразование Фурье, может быть использовано для сокрытия информации в графическом файле.

Одним из наиболее распространенных методов сокрытия информации в графических файлах является метод стеганографии. Он представляет собой процесс внедрения информации в графический файл, который является таким же, как и оригинальный файл, при этом информация внедряется в так называемые "незначимые" части файла, которые не влияют на внешний вид графического файла. Таким образом, стеганография позволяет передавать скрытые сообщения, не вызывая подозрений у третьих лиц.

В 2018 году сотрудник General Electric использовал фотографию заката чтобы украсть 40 файлов Excel и Matlab, содержащих данные, являющиеся коммерческой тайной.

Facebook манипулирует метаданными изображений, публикуемых на сайте, для отслеживания их дальнейшего распространения.

Цифровые стего-изображения так же встречаются в известной интернет-головоломке Цикада 3301, одним из основных фокусов которой является стегоанализ.

1.3. Разновидности методов сокрытия данных в цифровых изображениях.

1.3.1. LSB (Least Significant Bit - Наименее значимый бит)

Данный метод заключается в выделении наименее значимых бит изображения-контейнера с последующей их заменой на биты сообщения. Поскольку замене подвергаются лишь наименее значимые биты, разница между исходным изображением-контейнером и контейнером, содержащим скрытые данные невелика и обычно незаметна для человеческого глаза[1]. Метод LSB применим лишь к изображениям в форматах без сжатия (например, BMP) или со сжатием без потерь (например, GIF), так как для хранения скрытого сообщения используются наименее значимые биты значений пикселей, при сжатии с потерями эта информация может быть утеряна. Форматы без сжатия имеют очень большой размер и могут вызвать подозрение, поэтому для стеганографии чаще используют другие форматы.

Для внедрения, например, имеется чёрно-белое изображение, представленное в виде матрицы. Значения в этой матрице соответствуют яркостям пикселей, расположенных по координатам. Пусть эти значения представлены восьмибитными двоичными числами. Пусть скрываемое сообщение имеет размер 2 байта. Для хранения скрытого сообщения возьмём 2 младших бита изображения-контейнера. Тогда для сокрытия 2 байт, то есть 16 бит необходимо изображение размером минимум 8 пикселей. Если изображение содержит больше пикселей, чем необходимо для хранения сообщения, необходимо выбрать правило, по которому будут выбираться пиксели для встраивания данных. Этот закон должен быть заранее известен получателю, так как он будет необходим для извлечения данных. Для сокрытия факта встраивания данных, к неиспользованным пикселям изображения добавляется шум, чтобы шум, вносимый скрытыми данными, не выглядел аномальным. Например, имея изображение размером 4x2 пикселя запишем первые два бита сообщения 0001101100011011 в первый пиксель: пусть исходное значение пикселя 10100101, заменим младшие два бита на

первые два бита сообщения 10100100. Следующие два бита записываются в следующий пиксель, и так далее.

Для извлечения скрытых методом LSB данных, необходимо выбрать пиксели, содержащие полезную нагрузку по тому же закону, по которому они выбирались при встраивании. Далее, имея набор пар координат вида, по очереди, извлекаются наименее значимые биты: 10100100. Извлечённые биты данных объединяются, формируя скрытое сообщение.

1.3.2. PVD (Pixel Value Difference - Разность значений пикселей)

Этот метод учитывает тот факт, что на гладких участках (где значение яркости меняется незначительно) изменение будет более заметно, нежели на участках, содержащих более значительные перепады яркости.

Для внедрения исходное изображение разделяется на блоки по 2 пикселя, и скрытые данные кодируются как разность значений внутри этих блоков. Как и в случае с LSB, необходим закон, по которому будут выбираться блоки для встраивания. Для каждого используемого блока вычисляется модуль разности значений пикселей, по которому определяется диапазон допустимых значений. Чем больше перепад яркости внутри, блока- тем шире выбранный диапазон. Для удобства работы, ширина диапазона является степенью двух. Тогда, например, в блок с диапазоном шириной 4 можно записать 2 бита скрываемого сообщения (эти два бита, по сути, представляют собой выбор конкретного числа из диапазона). Блоки, изменение которых может привести к выходу за пределы допустимых значений яркости пикселей (от 0 до 255) не используются.

Для извлечения данных, изображение вновь делится на блоки по 2 пикселя. В соответствии с заранее известным правилом выбора блоков и последовательностью их обхода, для блоков рассчитывается разность значений пикселей и определяется диапазон, в который она попадает. Далее выполняется проверка на выход за пределы диапазона от 0 до 255: если при максимальной разности, входящий в диапазон, один из пикселей принимает значение больше 255 или меньше 0, то данный блок пропускается, так как он

был отброшен аналогичной проверкой на стадии встраивания. Из оставшихся блоков извлекаются данные: по ширине диапазона определяется количество бит, встроенных в блок, которые потом извлекаются, начиная с наименее значимого.

1.3.3. GLM (Grey Level Modification - Изменение уровня серого)

Метод GLM заключается в изменении чётности значения яркости изображения в чёрно-белом представлении. В каждый пиксель изображения встраивается 1 бит скрываемого сообщения.

Для встраивания в начале значения яркости всех пикселей делаются чётными, путём изменения всех нечётных значений на 1. Далее чётность этих значений сравнивается с чётностью битов данных. Например, если первый бит данных чётный (то есть равен 0), то первый пиксель не изменяется, если же он нечётный (равен 1), то значение яркости изменяется на нечётное.

Для извлечения для каждого пикселя, содержащего скрытое сообщение, определяется значение яркости. Если оно чётное, то соответствующий бит сообщения равен 0, если нечётное - то 1.

1.3.4. MPV (Mid Position Value - Значение в средней позиции)

В данном методе к изображению-контейнеру сначала применяется преобразование Арнольда, затем для каждого пикселя вычисляется его позиция. Для каждого оценивается количество знаков и положение среднего знака. Далее берётся число из позиции в и вычисляется ключ. Если это число превышает количество пикселей изображения, то берётся его остаток от деления на количество пикселей. Далее берётся десятичное значение последних 4 бит пикселя номер и вычисляется. В -й пиксель встраивается 2 бита данных по правилу: если четное, то применяется прямое встраивание, если нечётное, то обратное. Если чётное, то встраиваются два бита сообщения, нечётное - встраиваются комплементарные 2 бита. К полученному изображению применяется обратное преобразование Арнольда.

1.3.5. DCT (Discrete Cosine Transform - Дискретное косинусное преобразование)

Данный метод использует DCT-преобразование для перехода в частотную область и представляет собой LSB в применении к коэффициентам DCT. Поскольку сжатие JPEG так же использует DCT преобразование, то данную методику возможно применить к сжатым JPEG-изображениям. При использовании формата JPEG, встраивание производится после сжатия с потерями, использующего DCT, но до применения кода Хаффмана для дальнейшего сжатия коэффициентов DCT без потерь.

Для внедрения исходное изображение-контейнер разделяется на блоки по 8x8 пикселей, к которым применяется DCT. Из каждого коэффициента матрицы выделяются наименее значимые биты и заменяются на биты скрываемого сообщения.

Для извлечения изображение-контейнер разделяется на блоки по 8x8 пикселей, к которым применяется DCT. Из каждого коэффициента матрицы выделяются наименее значимые биты и объединяются, восстанавливая скрытое сообщение.

1.3.6. DWT (Discrete Wavelet Transform - Дискретное вейвлет-преобразование)

По своей сути данная методика схожа с основанной на DCT, но вместо DCT-преобразования для перехода в частотную область используется DWT-преобразование. Один из предложенных методов, основанных на DWT-преобразовании, предполагает определение областей изображения, содержащих цвет человеческой кожи в пространстве HSV, затем применяется DWT-преобразование и данные встраиваются только в эти области.

Глава 2. Реализация защиты от кражи информации через сокрытие ее в графических файлах.

2.1. Структура и описание организации.

ООО «DigitalGame» – организация в игровой индустрии, являющаяся одним из издателей игр. В соответствии с действующим законодательством, часть сведений, циркулирующих в ООО «DigitalGame», носит конфиденциальный и коммерческий характер, сведения подлежат защите для обеспечения сохранности: персональных данных сотрудников и игроков, коммерческой, служебной, профессиональной тайны и сведения о сущности проектов, которые находятся в разработке. Также информационные активы организации следует рассматривать как ценности организации, которые должны иметь гарантированную защиту (договоры с заказчиками, бухгалтерская отчетность, финансовая отчетность, юридическая документация, трудовые книжки и т.д.).

Московский офис организации ООО «DigitalGame» расположен в бизнес-центре “ Яуза-Тауэр” по адресу: г. Москва, ул. Радио, д. 24. Офис располагается на 4 этаже, под номером 411.

Офис состоит из следующих помещений (Приложение 1 - План офиса):

- отдел разработки;
- отдел тестирования;
- отдел кибербезопасности;
- отдел технической поддержки.

Также ЛВС состоит из следующих оборудований (Приложение 2 - План ЛВС офиса):

- 6 компьютеров;
- 6 коммутаторов;
- 3 серверов;
- 4 роутеров.

Организационная структура Московского офиса требует практичности и самостоятельности для эффективной работы с партнёрами, анализируется и актуализируется в соответствии с требованиями развития компании и рынка.

На рабочих станция предустановлено ПО под управлением ОС Windows. В отделе безопасности установлены дополнительные системы на ОС Linux. Развернута виртуальная инфраструктура ESXI для более гибкой работы персонала внутри и Active Directory с разграничением прав пользователей, службы сертификаций, DNS сервер. На рабочих станциях установлено антивирусное ПО Kaspersky Anti-Virus. Для сотрудников на удалённой работе, присутствует поднятый VPN сервер через OpenVPN. Для обеспечения безопасности передачи документов внутри компании используется носители СН “Секрет”.

2.2 Анализ существующих актуальных угроз безопасности информации в организации

Стеганография – метод скрытой передачи информации, который позволяет злоумышленникам передавать данные, не вызывая подозрений у посторонних. Хотя сама по себе стеганография не является угрозой безопасности, она может быть использована для незаконных или вредоносных целей. Далее рассмотрим несколько актуальных угроз безопасности информации, связанных с использованием стеганографии.

1. Утечка конфиденциальной информации: Злоумышленники могут использовать стеганографию для скрытой передачи конфиденциальных данных, таких как финансовые сведения, планы проектов или персональные данные сотрудников. Это представляет серьезную угрозу для безопасности информации в организации. Для защиты от этой угрозы необходимо регулярно обновлять системы защиты данных, внедрять политики контроля доступа и обучать сотрудников правилам безопасного обращения с конфиденциальной информацией.

2. Распространение вредоносного кода: Стеганография может быть использована для скрытой передачи вредоносных программ, таких как вирусы, трояны или шпионское ПО. Злоумышленники могут внедрять такие программы в носитель, например, в файлы изображений или звуковые файлы, обходя системы обнаружения вредоносного ПО. Для предотвращения этой угрозы рекомендуется использовать современные антивирусные программы, системы обнаружения вторжений и регулярно обновлять программное обеспечение с целью закрытия уязвимостей.

3. Обход систем обнаружения и блокировки: Злоумышленники могут применять стеганографию для обхода систем обнаружения и блокировки информации, установленных в организации. Это может позволить им обмануть системы фильтрации контента или обойти механизмы защиты от утечки информации. Для предотвращения этой угрозы рекомендуется установить и поддерживать актуальные системы защиты, проводить мониторинг и анализировать сетевой трафик, а также проводить регулярные аудиты систем безопасности.

Важно отметить, что сама стеганография не является незаконной или вредоносной, но ее злоупотребление может представлять угрозу для безопасности информации. Для эффективной защиты от подобных угроз рекомендуется использовать соответствующие меры безопасности, включая системы обнаружения вредоносного ПО, контроль доступа и обучение пользователям правилам безопасного обращения с информацией.

2.3 Оценка ущерба от реализации угроз

Примерная стоимость всех конфиденциальных данных, которая содержится в организации, составляет 20 00 000 рублей.

Конфиденциальная информация представляет из себя сведения:

- о разработке продукции;
- акциях;
- ведении торговли и оказании услуг;

- данные персонала;

- техническая документация.

Прямой финансовый ущерб от реализации угроз может оцениваться в 28 000 000 рублей. Ущерб от потери партнёров и репутации, будет составлять 3 000 000 рублей.

Потери от уменьшения стоимости ценных активов: 5 000 000 рублей.

Потери от неполучения доходов по неклиентским договорам: 17 договоров (общая сумма договоров - 24). Потери от невыполнения обязательств по договорам: 1 000 000 рублей.

Штрафы за нарушение законодательства: 400 000 рублей. Возможные потери в результате отзыва лицензий: 1 000 000 рублей.

Стоимость судебных издержек на дела по нарушению законодательства и условий договоров: 500 000 рублей. Затраты персонала на устранение последствий реализации угроз: 800 000 рублей.

Затраты на материалы/оборудования для устранения последствий реализации угроз будет превышать: 4 000 000 рублей.

2.4 Реализация стеганографических методов.

Когда дело касается стеганографии, обычно используется удивительный инструмент под названием Steghide в операционной системе Linux. Для его использования, нужно установить пакет steghide с помощью команды sudo apt-get install steghide.

Одна из самых интересных возможностей Steghide - это способность скрыть файлы в изображениях. Для этого помещается файл, который нужно скрыть, и изображение в одну директорию. Затем выполняется команда следующего вида:

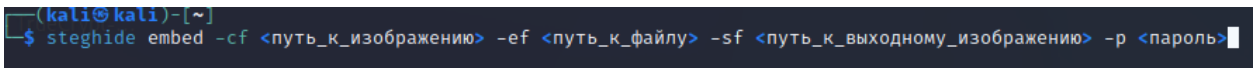

рис. 2.1. Внедрение текста в графический файл

<путь_к_изображению> нужно заменить на путь к изображению, <путь_к_файлу> на путь к файлу, который нужно скрыть,

<путь_к_выходному_изображению> на путь, по которому нужно сохранить измененное изображение, а <пароль> - это пароль, который выбирается для шифрования.

Чтобы извлечь скрытый файл из изображения, выполняется команда:

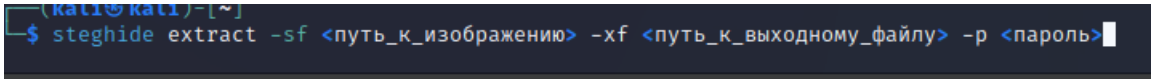

рис. 2.2. Извлечение текста из графических файлов

В этой команде <путь_к_изображению> - это путь к изображению, из которого нужно извлечь файл, <путь_к_выходному_файлу> - это путь, по которому нужно сохранить извлеченный файл, а <пароль> - это пароль, который использовался при скрытии файла.

2.5 Установка и настройка DLP-системы InfoWatch TrafficMonitor

Установка «все-в-одном» позволяет установить все компоненты Системы на один компьютер.

Чтобы установить Traffic Monitor Enterprise или Traffic Monitor Standard в режиме «Все-в-одном», выполните следующие действия:

1. Введите логин и пароль, чтобы войти в операционную систему (вход выполняется от имени пользователя root с использованием пароля, созданного при установке).
2. Создайте директорию, в которой будет располагаться инсталлятор InfoWatch Traffic Monitor. Например, для создания директории с именем distr в корне файловой системы выполните следующую команду:

mkdir /distr

3. Скопируйте в созданную директорию файлы, поставляемые в дистрибутиве InfoWatch

Traffic Monitor:

- iwtm-installer-x.x.x.xxx-rhel7.run (где x.x.x.xxx - номер сборки);
- iwtm-postgresql-9.6.19-x.xx.x.tar.gz;
- iwtm-oracle-12.2.0.1-x.xx.x.tar.gz;
- iwtm-adp-x.xx.x.tar.gz.

В нашем примере:

- iwtm-installer-7.1.0.229-rhel7.run;
- iwtm-postgresql-9.6.19-7.1.0.tar.gz; • iwtm-oracle-12.2.0.1-7.1.0.tar.gz; • iwtm-adp-7.1.0.tar.gz.

4. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor. В нашем примере:

cd /distr

5. Выполните следующую команду:

bash ./iwtm-installer-x.x.x.xxx-rhel7.run В нашем примере команда будет следующей: bash ./iwtm-installer-7.1.0.229-rhel7.run

Начнется распаковка файлов, необходимых для установки Traffic Monitor. Перед запуском установщик выполнит проверку Системы и, если будет обнаружено несоответствие требованиям, прервет установку, выведя сообщение об ошибке. В этом случае необходимо исправить указанное установщиком несоответствие и повторно запустить установку.

По завершении на экране отобразится окно с приглашением установить Traffic Monitor

(номер в окне соответствует номеру устанавливаемой версии Системы)

рис. 2.3. Приветственное окно InfoWatch

Для продолжения нажмите Continue.

6. В окне выбора редакции Traffic Monitor укажите:

- TM Enterprise – для установки редакции Enterprise;
- TM Standard – для установки редакции Standard.

Для этого установите знак астериска (*) в поле редакции и нажмите пробел, затем - OK.

7. В окне выбора базы данных укажите, какая СУБД должна быть установлена (опция доступна только для TM Enterprise):

- Oracle;
- PostgreSQL.

Для этого установите знак астериска (*) в поле напротив выбранной СУБД, используя клавишу пробел, и нажмите OK.

8. Если была выбрана редакция TM Enterprise, в окне выбора режима установки выберите All-in-one.

Для этого установите знак астериска (*) напротив выбранного режима, используя клавишу пробел, затем нажмите OK.

9. Введите название дата-центра Consul и нажмите OK.

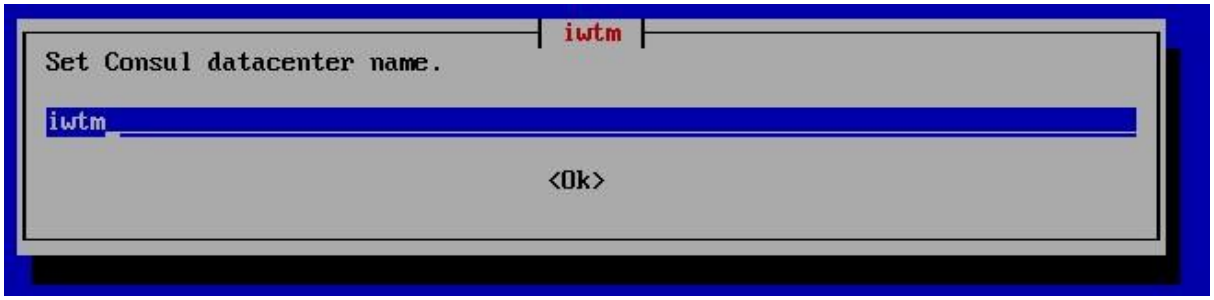

рис. 2.4. Установка названия дата-центра Consul

10. Настройте адрес сервера для синхронизации времени (NTP-server). Для этого с помощью клавиши пробел установите знак астериска (*) в поле DNS, затем нажмите OK.

11. Настройте параметры локализации

12. Настройте параметры хранения данных в БД Системы

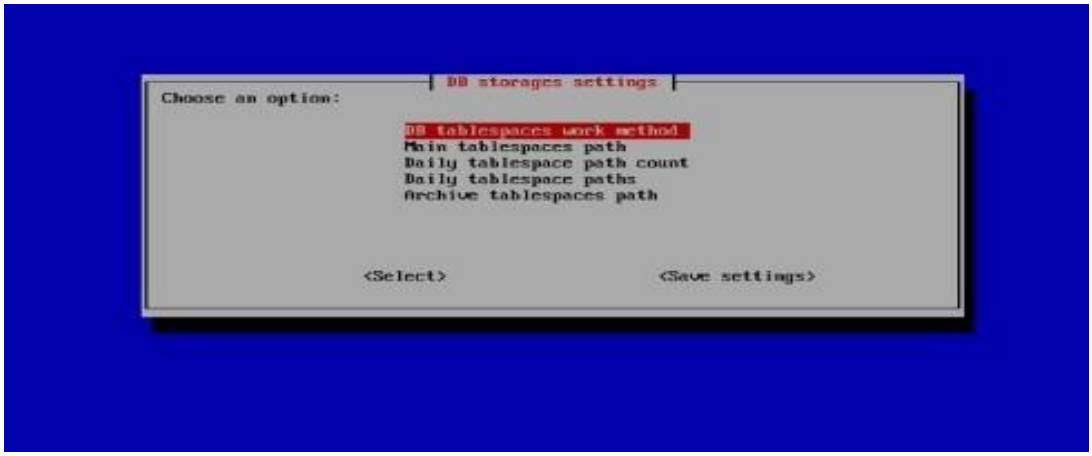

рис. 2.5. Настройка параметров хранения данных в базе данных системы

Определите режим хранения файлов табличного пространства, установив знак астериска (*) в поле напротив выбранного режима, и нажмите OK.

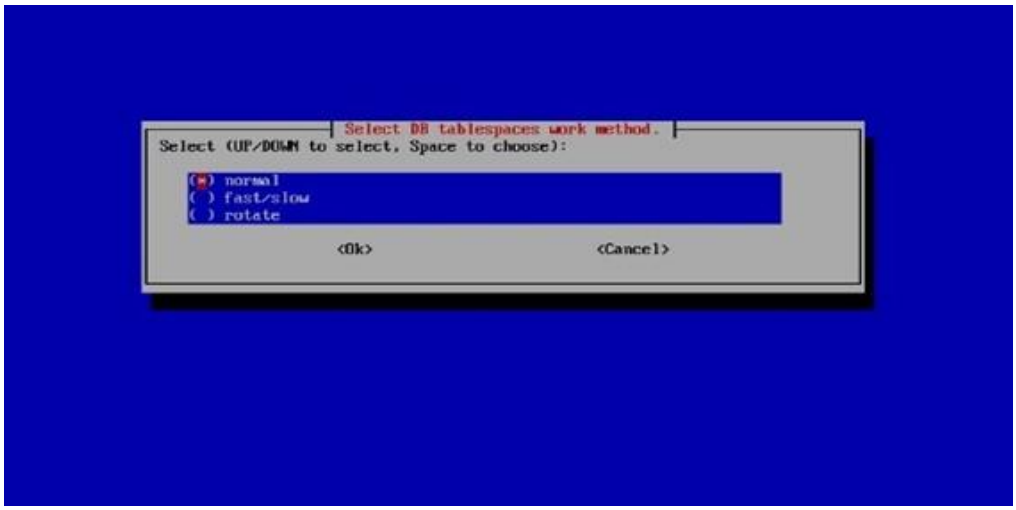

рис. 2.6. выбор режима хранения файлов табличного пространства

13. Настройте параметры автоматического удаления событий из БД (по умолчанию автоматическое удаление отключено):

- Выберите Events cleaning и нажмите select:

- При необходимости вы можете выбрать несколько пунктов.

- Нажмите Ok.

- Если включено автоматическое удаление событий с нарушением, укажите период их хранения до удаления:

- Выберите Violation и нажмите Select:

- В открывшемся окне введите количество дней, по прошествии которых событие будет автоматически удаляться (по умолчанию: 90 дней).

- Нажмите Ok.

- Если включено автоматическое удаление событий без нарушения, укажите период их хранения до удаления:

- Выберите Non-violation и нажмите Select:

- В открывшемся окне введите количество дней, по прошествии которых событие будет автоматически удаляться (по умолчанию: 45 дней).

- Нажмите Ok.

- Если включено автоматическое удаление снимков экрана, полученных от Агентов Device Monitor, укажите период их хранения до удаления:

- Выберите Screenshots и нажмите Select:

- В открывшемся окне введите количество дней, по прошествии которых снимки экрана будут автоматически удаляться (по умолчанию: 90 дней).

- Нажмите Ok.

- По завершении настроек нажмите Save settings.

- В открывшемся окне проверьте, что все настройки указаны правильно, затем нажмите Yes.

Начнется установка СУБД и схемы БД. Прогресс выполнения будет отображаться на экране.

В результате установки в системе будут созданы учетные записи, приведенные в статье "Предустановленные серверные параметры".

Установка Веб-консоли управления происходит в автоматическом режиме с помощью программы инсталлятора. После окончания установки серверных компонентов работа в консоли управления доступна через окно браузера, при этом требуется ввести URL-адрес сервера Traffic Monitor.

2.6 Создание политики запрета передачи графических изображений.

В самом начале нужно настроить технологии, которые будут обнаруживать требуемые данные.

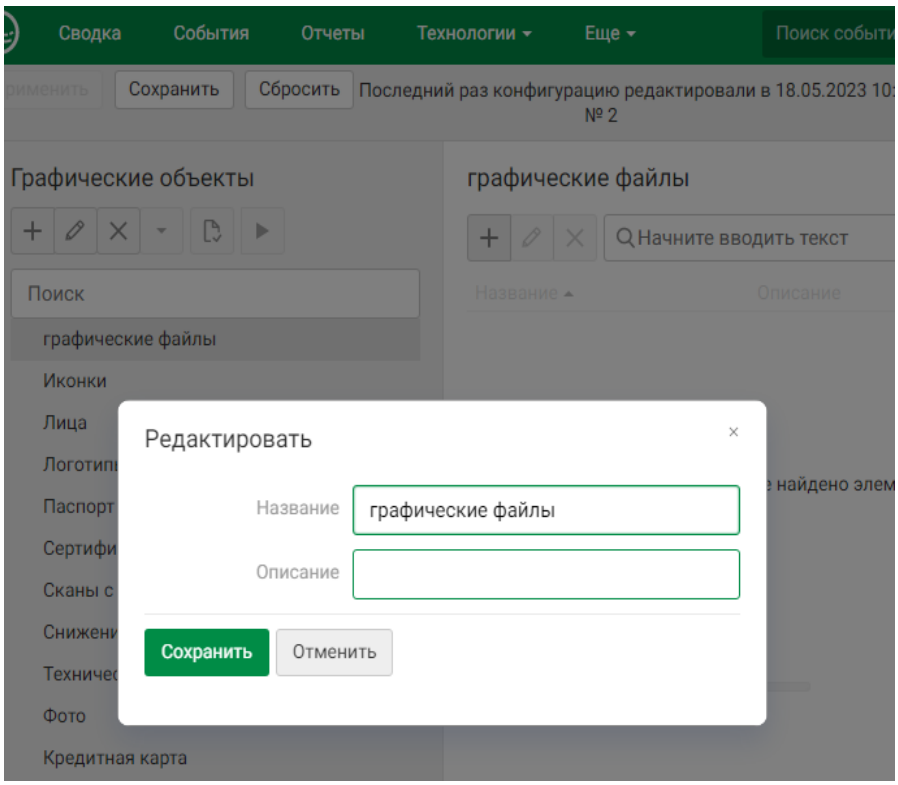

рис. 2.7. создание и настройка технологий

Нужно в верхней зеленой навигационной панели выбрать пункт «Технологии», далее выбрать «графические объекты», в открывшемся окне в левой части будет иконка «+» что означает добавить, в открывшемся инлайн окне написать название и описание, а потом сохранить его.

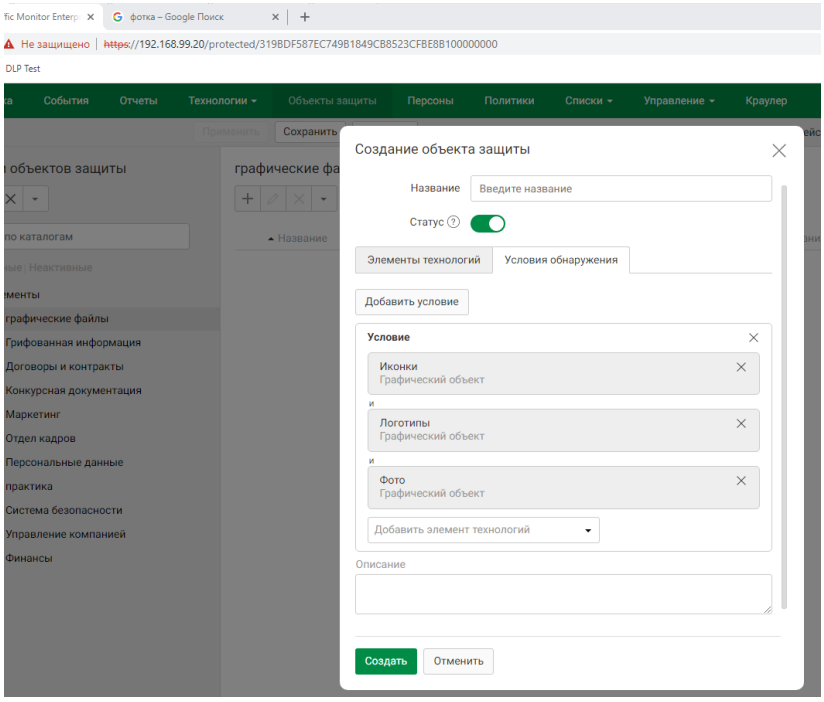

Рис. 2.8. создание объекта защиты

Следующим действием будет создание объекта защиты.

В верхней зеленой навигационной панели нужно выбрать пункт «Объекты защиты», потом в открывшемся окне в левой части нажать иконку «+» и назвать объект защиты и выбрать из технологий созданную ранее технологию «графические файлы» и нужно добавить условие при которых будет срабатывать наша политика (в нашем случае выбираем все графические файлы).

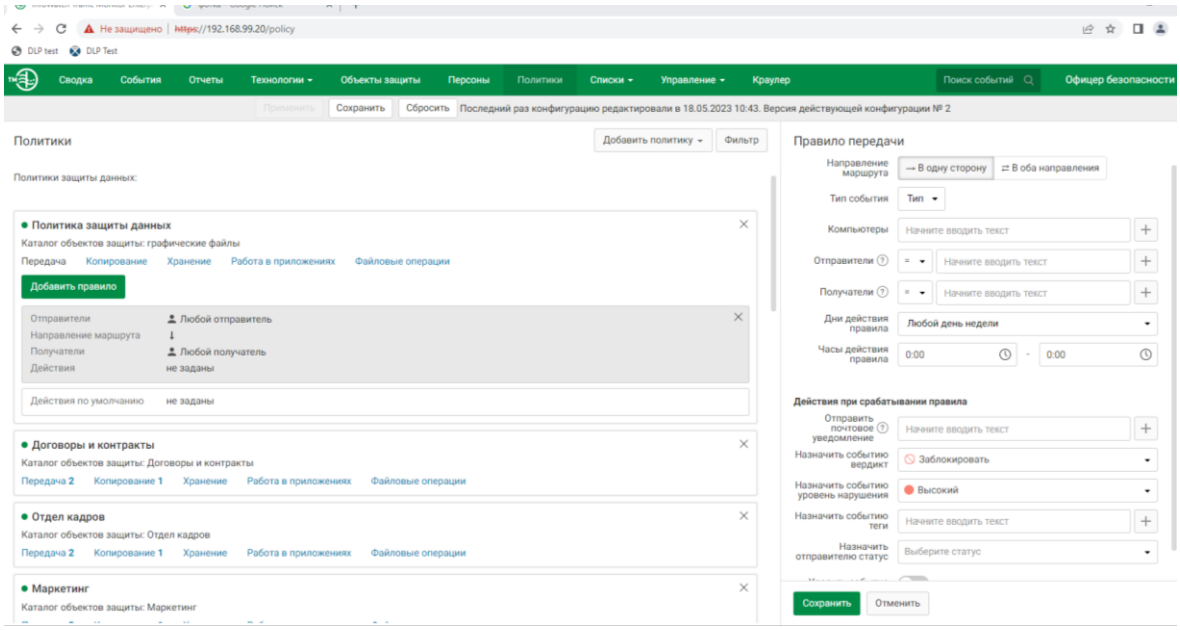

Рис. 2.9. создание и настройка политики безопасности

Следующим шагом мы настраиваем уже саму политику безопасности, которая будет реагировать на передачу графических файлов.

Нужно в верхней зеленой навигационной панели выбрать пункт «политики», далее «добавить политику» и выбрать «Политика защиты данных» и ранее созданный объект защиты, далее в пункте передача выбрать «добавить плавило», далее в пункте «действия при срабатывании правила» выбрать «заблокировать» в пункте «назначить событию вердикт» и «высокий» в пункте «Назначить событию уровень нарушения».

Таким образом была настроена политика на запрет передачи графических файлов на предприятии.

Заключение

В рамках данной курсовой работы были исследованы различные аспекты сокрытия информации в графических файлах с использованием стеганографии. Основной целью работы было изучение техник и инструментов, которые позволяют осуществлять скрытое встраивание данных в изображения, а также их извлечение.

В процессе исследования были рассмотрены основные принципы работы стеганографии и ее применение в контексте безопасности информации. Были изучены различные методы сокрытия данных в графических файлах, такие как метод LSB (Least Significant Bit) и метод модификации частотного спектра. Каждый из методов имеет свои преимущества и ограничения, и выбор конкретной техники зависит от требуемого уровня безопасности и возможных ограничений при передаче или хранении данных.

Кроме того, были проанализированы различные инструменты для работы с сокрытием информации в графических файлах, включая популярную утилита, такую как Steghide. Этот инструмент предоставляет широкий набор функций для встраивания и извлечения данных, а также позволяет задавать параметры шифрования и стеганографические методы.

Исследование показало, что сокрытие информации в графических файлах имеет широкий спектр применений, включая обеспечение конфиденциальности, контроль доступа и цифровую подпись. Однако при использовании стеганографии необходимо учитывать потенциальные угрозы безопасности, такие как возможность утечки конфиденциальных данных или распространение вредоносного кода.

В ходе курсовой работы была внедрена DLP-система от InfoWatch и настроена политика на запрет передачи графических файлов.

Список литературы

https://ru.wikipedia.org/wiki/Стеганография

https://www.kaspersky.ru/resource-center/definitions/what-is-steganography

https://habr.com/ru/articles/253045/

Коржик В. И. Цифровая стеганография и цифровые водяные знаки [Текст] / В. И. Коржик // СПбГУТ, 2017.

Окатов А.В. Методы цифровой стеганографии [Текст] / А. В. Окатов // ГУАП, 2016.

Рябко Б.Я. Криптография и стеганография в информационных технологиях [Текст] / Б. Я. Рябко, А. Н. Фионов, Ю. И. Шокин // Наука, 2015.