Лабораторная работа № 12
Сокрытие информации методом временного распыления

1. Цель работы

Получить навыки в использовании метода пространственно-временного распыления информации, ознакомиться с возможностями языков программирования JavaScript и HTML.

2. Общие сведения

При использовании принципа временного распыления информации блоки сообщений передают по каналам связи в псевдослучайные моменты времени, причём для уменьшения вероятности перехвата продолжительность передачи фрагмента сообщения устанавливают минимально возможной, но достаточной для принимающей стороны. Расписание передачи информации (временные окна) определяется корреспондентами с помощью ключа. Передачу информационных блоков в канале связи перемежают трансляцией информационно пустых (маскирующих) блоков.

Идею передачи информации по расписанию рассмотрим на примере использования для связи глобальной сети Internet. Программную реализацию принципа временного разделения сообщения можно осуществить с помощью различных языков программирования (JavaScript, Perl, PHP, Java и т.д.).

Рассмотрим, как выполнить временное распыление с помощью языка программирования JavaScript. Приведённый ниже скрипт позволяет кратковременно заменять фотографию const.jpg на фотографию secret.jpg. В данном случае замена будет происходить в 17 часов 18 минут 35 секунд, а обратная замена - в 17 часов 19 минут 26 секунд. Передаваемое сообщение предварительно скрыто размещают в контейнере secret.jpg.

```
<script language="JavaScript">
var start = new Date();
var end = new Date();
start.setHours(17);
start.setMinutes(18);
start.setSeconds(35);
end.setHours(17);
end.setMinutes(19);
end.setSeconds(26);
var now = new Date();
st = start.getTime();
et = end.getTime();
time = now.getTime();
if ((time >= st) && (time < et)) document.write("<img
```

```
src=\"secret.jpg\">");
        else document.write("<img src=\"const.jpg\" >");
        </script>
```

В рассмотренном примере демонстрация секретной информации на Web-странице происходит в течение короткого времени. Внешне две демонстрируемые фотографии должны быть одинаковыми (объекты-близнецы). Однако фотография secret.jpg является стегоконтейнером и содержит в себе скрытую информацию.

Приведённый пример иллюстрирует идею временного распыления информации. Но проводить практическую реализацию этой идеи с помощью JavaScript нежелательно. Недостатком подобной защиты сообщения является имеющаяся у криптоаналитика возможность ознакомления с кодом скрипта, за счёт чего он в состоянии определить момент демонстрации (передачи) стегоконтейнера. Просмотр текста программы осуществляется стандартным путём с помощью любого браузера. Этот недостаток присущ всем скриптам, исполняемым на клиентской ЭВМ. Однако даже при имеющейся возможности по коду скрипта установить время подмены контейнеров у криптоаналитика остаётся нерешённой задача определения доменного адреса (IP-адреса) Web-страницы, на которой размещён стегоконтейнер. Доменные адреса используемых Web-страниц известны только корреспондентам. Выбор корреспондентами используемых серверов и Web-страниц (каналов связи) осуществляется с помощью ключа.

Рассмотрим пример реализации этой же идеи с помощью языка программирования PHP. Следующий скрипт заменяет в 10 часов 47 минут Web-страницу page2.html страницей page1.html, которая является стегоконтейнером. Через минуту происходит обратная замена.

```
        <?php
        // формат ччмм
        //Установка времени начала демонстрации стегоконтейнера
        $start_time = '1047';
        //Установка времени конца демонстрации стегоконтейнера
        $end_time = '1048';
        //Считывание текущего времени
        $now_time = date('Gi');
        //Сравнение текущего времени с моментами начала и конца демонстрации
        if ($now_time >=$start_time && $now_time <$end_time) {
        //Загрузка страницы, содержащей скрытые данные
        header('location:page1.html');
        exit;
        }
        else {
```

```
//Загрузка маскирующей страницы
header('location:page2.html');
exit;
}
?>
```

Повышение криптостойкости в результате применения принципа временного распыления сообщения происходит за счёт того, что за определённое время может осуществляться многократная подмена оригинального объекта различными объектами-близнецами, но только контейнер, переданный в заранее обусловленное время, содержит полезную для получателя информацию. При этом маскирующие объекты-близнецы могут содержать дезинформацию (вложение в контейнере есть, но оно не относится к передаваемому сообщению).

Рассмотренный принцип легко развить и усовершенствовать, например, можно на одной Web-странице сразу демонстрировать несколько стего-контейнеров (рисунки, тексты, фотографии, видео) и передавать не один блок информации за определённый промежуток времени, а несколько. Другими словами, пространственно-временное распыление информации можно вести не только по каналам связи, но и по контейнерам. При этом блоки разных сообщений целесообразно переставлять и передавать их не последовательно, а в псевдослучайном порядке. Это повышает вычислительную сложность криптоанализа.

Скрипты, написанные на языке PHP, являются серверными приложениями, поэтому криптоаналитик не может самостоятельно получить листинги программ и на основе анализа кода определить, в какое время происходит подмена объекта. Обнаружить подмену можно по изменяющемуся содержимого контейнера, но для этого придётся непрерывно контролировать множество Web-страниц. Сложность пеленгации Web-страницы состоит ещё и в том, что доменный адрес криптоаналитику неизвестен, а до момента обнаружения роботом поисковой системы нового доменного адреса проходит несколько дней.

Технологически надёжно реализовать непрерывный мониторинг большого числа Web-страниц сложно. Это требует от криптоаналитика существенных капитальных и эксплуатационных вложений. Таким образом, временное распыление– это технологический барьер, сложность преодоления которого состоит в необходимости непрерывного контроля множества Web-страниц, для чего требуется использование вычислительных средств большой мощности.

3. Задания на выполнение лабораторной работы

3.1. Задание 1. Сокрытие текста в графическом контейнере

В соответствии с вариантом с помощью программы S-Tools скрыть заданный текст в графическом файле формата BMP. Графический файл (пустой контейнер) следует выбрать из папки **Контейнеры**, причём имена папок и файлов совпадают с номерами вариантов (например, для первого варианта нужно выбрать файл 1.bmp). Пароль и метод шифрования нужно выбрать самостоятельно.

Таблица3.1.1

Вар	Текст
1	Время приближается медленно, а уходит быстро.
2	Не количество жизни дорого, а качество.
3	На крыльях времени уносится печаль.
4	Время проходит, но сказанное слово остаётся.
5	Есть люди, которые крайне пунктуально опаздывают.
6	Не думай о секундах свысока. Наступит время - сам поймёшь…
7	Время – деньги. Две недели – уже аванс.
8	Время – самое драгоценное из всех средств.
9	Ничто так не торопит, как вечность.
10	Все приходит в своё время для тех, кто умеет ждать
11	Опасайся тех, кто сетует на нехватку времени, - они крадут твоё.
12	Минуты длительны, а годы скоротечны.
13	Праздный человек есть животное, поедающее время.
14	Время – это капитал работника умственного труда.
15	Пока мы думаем как убить время, время убивает нас.
16	Чтобы научиться ценить минуты, нужны годы.
17	День дорог для того, кто умеет жить.

3.2. Задание 2. Исследование метода временного распыления информации

Разместить на Web-странице четыре фотографии формата JPEG, одна из которых в определённое время должна быть заменена фотографией формата BMP, начинённой секретной информацией (из задания 3.1). Имя заменяемой фотографии, а также интервал времени, на который должна появляться начинённая фотография, выбирается в соответствии с таблицей 3.2.1. Для создания Web-страницы следует использовать шаблона index.html (см. папку 17, а также Приложение 5). Фотографии для Web-страницы находятся в папке **Контейнеры**. Подобно первому заданию имена папок совпадают с номерами вариантов. На странице должно быть указано: время выполнения задания, фамилия, имя студента, группа и номер варианта.

Таблица 3.2.1

Вар	Имя заменяемого файла	Интервал времени появления секретной информации, минут
1	5.jpg	4
2	4.jpg	3
3	1.jpg	2
4	2.jpg	5
5	3.jpg	8
6	5.jpg	1
7	4.jpg	2
8	1.jpg	5
9	2.jpg	6
10	3.jpg	3
11	5.jpg	7
12	4.jpg	6
13	1.jpg	6
14	2.jpg	5
15	3.jpg	2
16	4.jpg	1
17	5.jpg	1

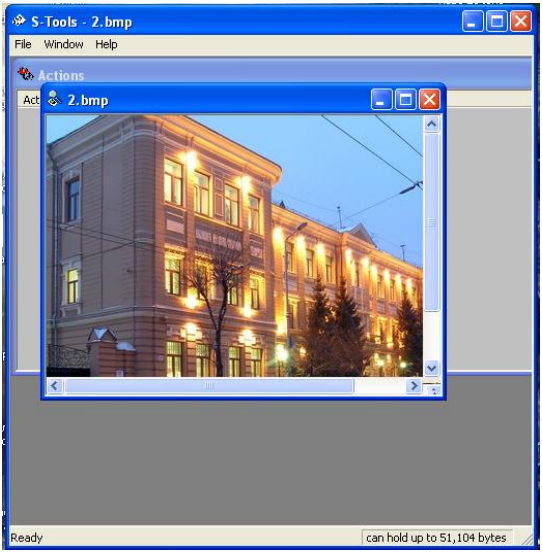
4. Порядок выполнения лабораторной работы

4.1. Методические указания к заданию 3.1

Описание порядка выполнения этого задания рассмотрим на примере варианта 17.

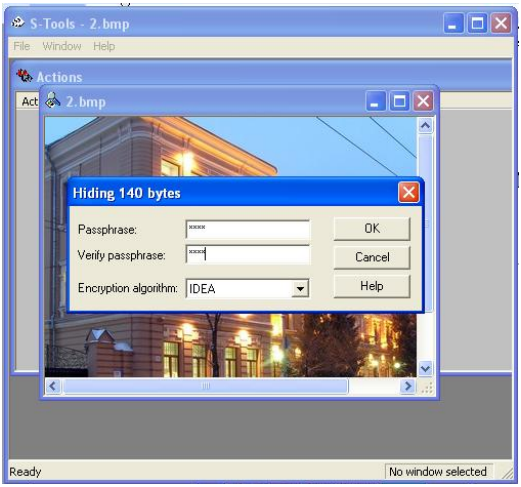
Для сокрытия текста в графическом файле формата BMP с помощью программы S-Tools нужно выполнить следующие действия.

В папке **Контейнеры** найти папку, имя которой совпадает с номером варианта (в данном случае 17), затем «перетащить» мышью файл 2.bmp в открытое окно программы S-Tools.



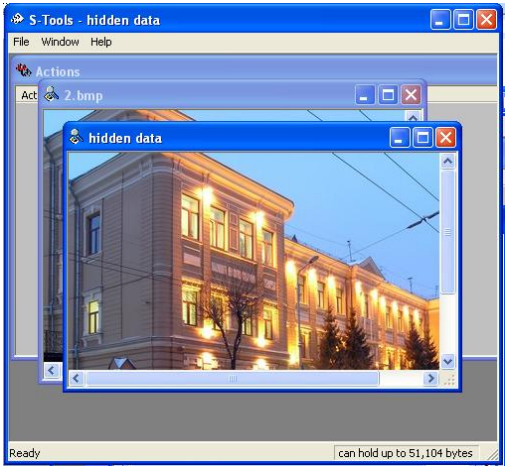
Затем «перетащить» txt-файл с текстом «День дорог для того, кто умеет жить» в окно файла-контейнера. Заметим, что максимально возможный размер скрываемой информации указан в нижнем правом углу окна S-Tools.

Если размер файла достаточен для сокрытия данных в нём, то появится новое окно. В нём следует ввести пароль (**Passphrase**), подтвердить его (**Verify Passphrase**), а также выбрать алгоритм шифрования (**Encryption Algorithm**).

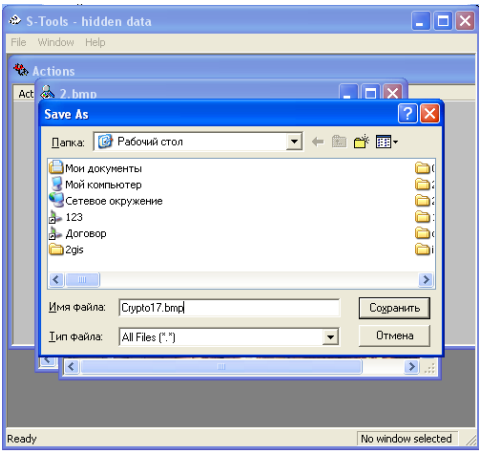


Затем появится меню задания свойств (для изображений) - **Convert to a 24-bit** image (Конвертировать в 24-битное изображение) или **Attempt colour reduction** (Уменьшение цветовой гаммы).

Результат преобразования появится в окне **Hidden data** (Скрытые данные).



Для сохранения результатов шифрования, нужно щелчком правой кнопки мыши выбрать опцию **Save as…** (Сохранить как…), указать имя файла, расширение, и выбрать месторасположение. Целесообразно сохранить файл с именем crypto17.bmp, где 17 - это номер варианта.



Этот файл с зашифрованной и скрытой информацией будет использоваться в следующем задании.

4.2. Методические указания к заданию 3.2

Рассмотрим пример выполнения задания по варианту 17.

Вначале необходимо с помощью Notepad (Блокнот) открыть страницу-шаблон index.html. Далее нужно сделать правку документа таким образом, чтобы на Web-странице были указаны фамилия и имя студента, его группа, номер варианта.

Для выполнения правки Web-страницы следует выполнить следующие действия.

В строке <H5 align=right><B> Студент группы
Вариант № </B></H5> после слова «Студент» добавить свою фамилию и имя, после слова «группы» добавить номер своей группы, после фразы «Вариант №» добавить номер варианта.

Следом за этим нужно в папке **Контейнеры** найти папку, имя которой совпадает с номером варианта (в рассматриваемом примере 17), выяснить какие рисунки должны появиться на странице (в рассматриваемом случае это файлы 1, 3, 4, 5). Подписи должны соответствовать изображениям, что также выполняется путём изменения скрипта.

В строке <td align="center"><H4><B>ГазБанк</B></H4> между тегами <B></B> вписать название первой фотографии.

В строке <IMG src="1.jpg" width=300> указать имя файла с первой фотографией, width=300 – определяет ширину фотографии.

Аналогично делаются изменения в строках – <td align="center"><H4><B>НомосБанк</B></H4> <IMG src="3.jpg" width=300, <td align="center"><H4><B>СберБанк на ул. Гагарина</B></H4> <IMG src="4.jpg" width=300>.

Найти фрагмент кода if ((time >= st) && (time < et)) document.write("<H4 align=center><B>ГУ СберБанк</B></H4><P align=center><img src=\"2.bmp\" width=150</P>") и в нем также сделать подобные изменения, учитывая, что он отвечает за появление фотографии со скрытыми данными.

Строка else document.write("<H4 align=center><B>АвтоВазБанк</B> </H4 ><P align=center><img src=\"5.jpg\" width=300</P>") отвечает за исчезновение изображения 5.jpg, здесь также требуется внести изменения в название фотографии и имени файла.

Следующим действием производится замена фотографии на определённый промежуток времени. В рассматриваемом примере требуется замена фотографии 5.jpg на фотографию crypto17.bmp на время, равное одной минуте (таблица 3.2.1).

Для варианта 17 нужно сделать следующие исправления в листинге программы:

В строке start.setHours(23) поставить час исчезновения изображения 5.jpg и появления фотографии 2.bmp, в start.setMinutes(52) – минуту исчезновения.

В строке end.setHours(23) указать час исчезновения фотографии 2.bmp и появления фотографии 5.jpg, в end.setMinutes(53) – минуту.

В данном случае получилось, что в 23.52 исчезает изображение 5.jpg и появляется 2.bmp, а в 23.53 5.jpg обратно заменяет 2.bmp.

В итоге листинг программы будет иметь вид:

```
<html>
<head>
<table align="center" width="100%" cellpacing="0" cellpadding="0" bor-
der="3">
<tr>
<td>
<body leftmargin=0 topmargin=0>
<script language="JavaScript">
cDate = new Date();
document.write("Время выполнения задания: "+ cDate.toLocaleString());
</script>
</body>
</td>
</tr>
<tr>
<td COLSPAN=4>
<H5 align=right><B> Студент группы <BR> Вариант №
</B></H5>
</td>
</tr>
<tr>
```

```
<td COLSPAN=4><H2 align=center><B> Сокрытие информации методом временного
 распыления</B></H2>
</td>
</tr>
<tr>
<td align="center"><H4><B>ГазБанк</B></H4>
<IMG src="1.jpg" width=300>
</td>
<td align="center"><H4><B>НомосБанк</B></H4>
<IMG src="3.jpg" width=300
</td>
</tr>
<tr>
<td align="center"><H4><B>СберБанк на ул. Гагарина</B></H4>
<IMG src="4.jpg" width=300>
</td>
</head>
<body>
<td>
<script language="JavaScript">
  var start = new Date();
  var end = new Date();
  start.setHours(23);
  start.setMinutes(52);
  end.setHours(23);
  end.setMinutes(53);
  var now = new Date();
  st = start.getTime();
  et = end.getTime();
  time = now.getTime();
  if ((time >= st) && (time < et)) document.write("<H4 align=center><B>ГУ СберБанк</B></H4><P align=center><img src=\"2.bmp\" width=150</P>");
else document.write("<H4 align=center><B>АвтоВазБанк</B> </H4 ><P align=center><img src=\"5.jpg\" width=300</P>");
</script>
</td>
</body>
</tr>
</table>
</html>
```

Примечание.

Для наблюдения за сменой изображений необходимо в моменты сме-

ны изображений нажать клавишу обновления (F5).

5. Требования к отчёту

Отчёт подготавливается в электронном виде. В нём описывается порядок выполнения заданий. В отчёте необходимо указать максимально допустимый объем скрываемой информации в указанном графическом файле, описать порядок сокрытия текстового файла в графическом контейнере с помощью программы S-Tools, а также привести выбранный алгоритм шифрования и пароль. Отчёт должен содержать листинг программы на языке JavaScript со сделанными исправлениями.

6. Контрольные вопросы

6.1. Для чего предназначена программа S-Tools?
6.2. Приведите примеры контейнеров, которые могут быть использованы для скрытой передачи информации.
6.3. Какова структура Web-страницы?
6.4. Что располагается между тегами <body>< /body >?
6.5. С помощью каких тегов создаётся таблица?
6.6. Как восстановить данные, скрытые программой S-Tools в графическом файле?
6.7. Как сделать выравнивание текста в абзаце?
6.8. Какой тег отвечает за отображение иллюстрации на странице?
6.9. Какой объект отвечает за отображение времени?
6.10. Как объединить несколько ячеек в таблице?
6.11. Поясните строки программы, отвечающие за смену изображения.
6.12. Как сделать разметку страницы невидимой?

7. Список литературы

1. Алексеев А.П., Сухова Е.Н. Передача скрытых сообщений методами стеганографии. Мет. указания на проведение лабораторных работ. Самара: ПГАТИ, 2003. - 19 с.

2. А.П. Алексеев. Метод пространственно-временного распределения информации. XVI Российская научная конференция профессорско-преподавательского состава, научных сотрудников и аспирантов. - Самара, ПГУТИ, 2009 г., стр. 167-168.

3. Алексеев А.П., Жеренов Ю.В. Сокрытие информации методом временного распыления. Мет. указания на проведение лаб. работ. Самара: ПГУТИ, 2010. -16 с.