

Министерство общего и профессионального образования Ростовской области
государственное бюджетное профессиональное образовательное учреждение Ростовской области
«Ростовский-на-Дону колледж связи и информатики»
(ГБПОУ РО «РКСИ»)

ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

по специальности

09.02.03 «Программирование в компьютерных системах»

Студент Юнашева Екатерина Павловна

(Фамилия, имя, отчество)

Курс 4 Группа ПОКС-49

Общепрофессиональная дисциплина:
ОП.14 «Информационная безопасность»

Преподаватель колледжа:

_____ О.П. Манакова

Студент:

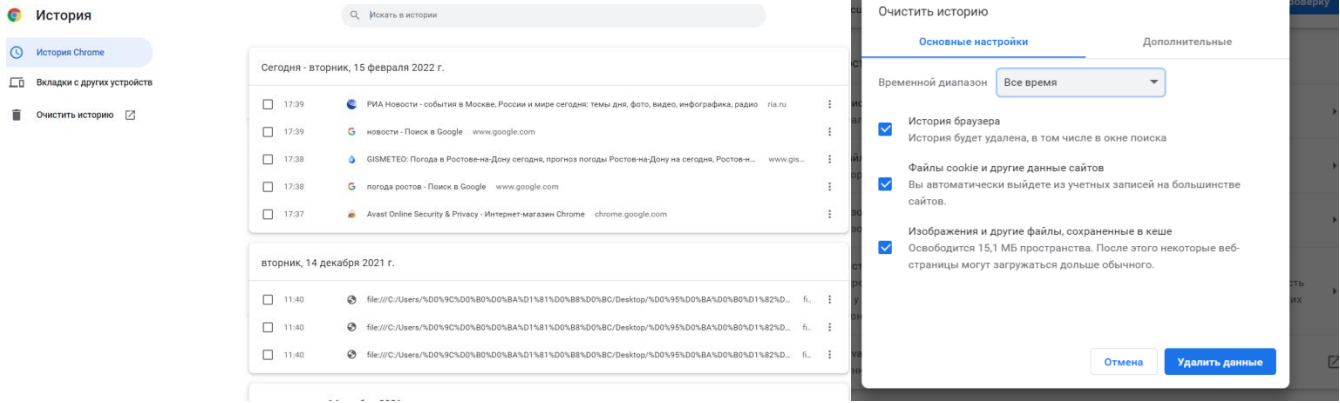
_____ Е.П. Юнашева

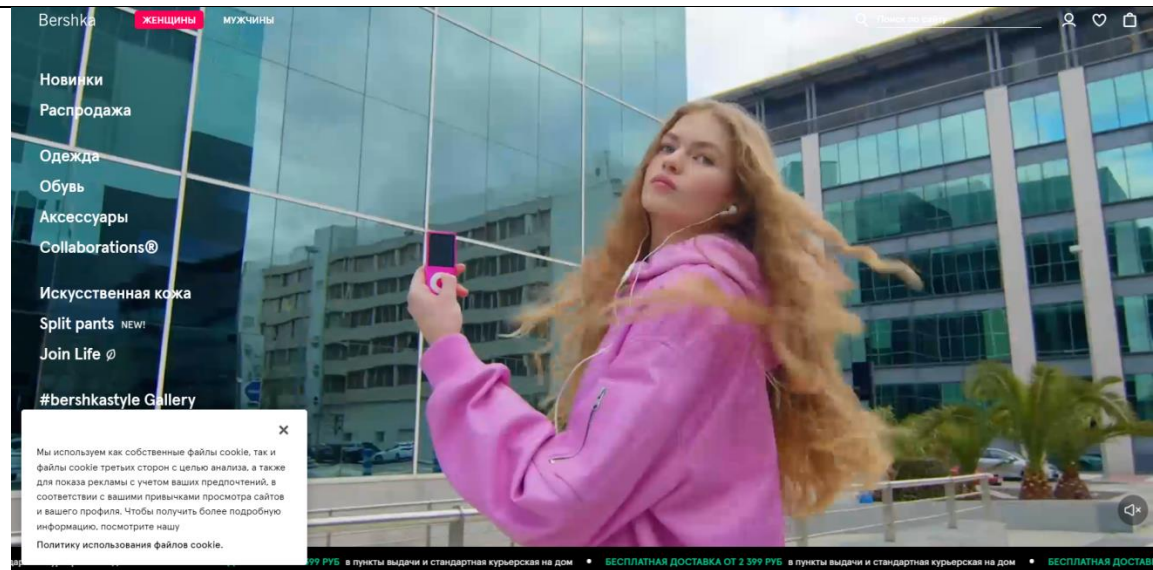
Ростов-на-Дону

2021-2022 уч. г.

Практическое занятие №1

1. Наименование практического занятия: Настройки безопасности и конфиденциальности в браузере.
2. Цели практического занятия: Исследовать настройки безопасности и конфиденциальности в браузере.
3. Количество часов: 2
4. Место проведения: главный корпус РКСИ, ауд. 420.
5. Перечень используемого оборудования: компьютер, выход в глобальную сеть, комплект учебно-методической документации, раздаточный материал, операционная система MSWindows, браузер GoogleChrome.
6. Последовательность проведения работ:

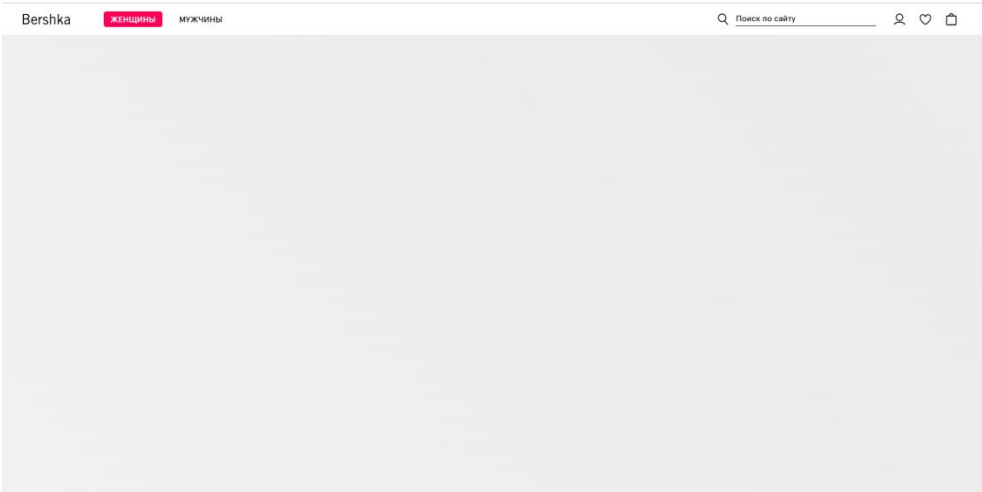
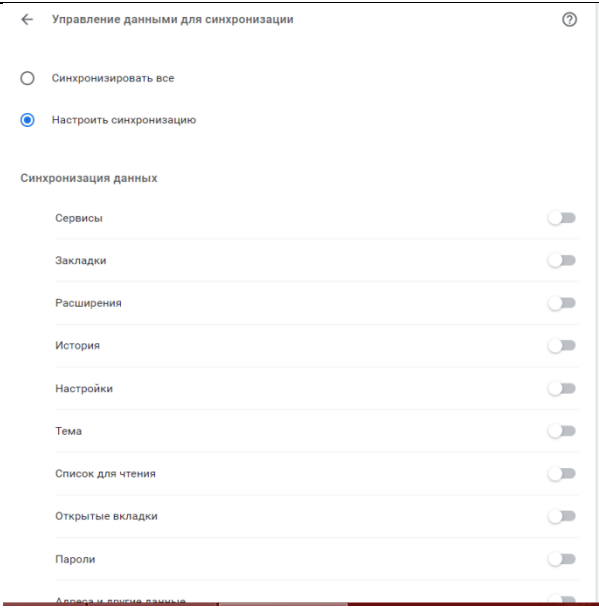
№ п/п	Этап выполнения задания	Описание выполняемых работ
1	Очистить кэш и куки в браузере.	 <p>The screenshot shows the Google Chrome 'История' (History) page on the left, displaying a list of visited websites and their timestamps. On the right, the 'Очистить историю' (Clear browsing data) dialog box is open, showing the 'Основные настройки' (Basic settings) tab. The 'Временной диапазон' (Time range) is set to 'Все время' (All time). The 'История браузера' (Browser history) checkbox is checked, and the 'Файлы cookie и другие данные сайтов' (Cookies and other site data) checkbox is also checked. The 'Изображения и другие файлы, сохраненные в кеше' (Images and other files stored in cache) checkbox is checked, with a note indicating that 15.1 MB of space will be freed. The 'Удалить данные' (Delete data) button is highlighted in blue.</p>
2	Найти сайты требующие работу с куки и проверить их работу (скорость загрузки, правильность отображения контента) при отключенных куки в браузере (интернет-магазины, погода и т.п.).	Отображение сайта с включенными куки:




Общие настройки

<input type="radio"/>	Показать все файлы cookie	▼
<input type="radio"/>	Блокировать файлы cookie сторонних сайтов в режиме инкогнито	▼
<input type="radio"/>	Блокировать сторонние файлы cookie	▼
<input checked="" type="radio"/>	Заблокировать все файлы cookie (не рекомендуется)	▲
<input checked="" type="checkbox"/>	Сайты не могут использовать файлы cookie, чтобы сделать работу в браузере более удобной, например запоминая товары в корзине или информацию о том, что вы вошли в аккаунт	
<input checked="" type="checkbox"/>	Сайты не могут использовать файлы cookie, чтобы отслеживать ваши действия в браузере, например, для показа персонализированной рекламы.	
<input checked="" type="checkbox"/>	Функции многих сайтов могут стать недоступными	
Удалять файлы cookie и данные сайтов при закрытии всех окон		<input type="checkbox"/>
Отправлять запрет на отслеживание для исходящего трафика		<input type="checkbox"/>

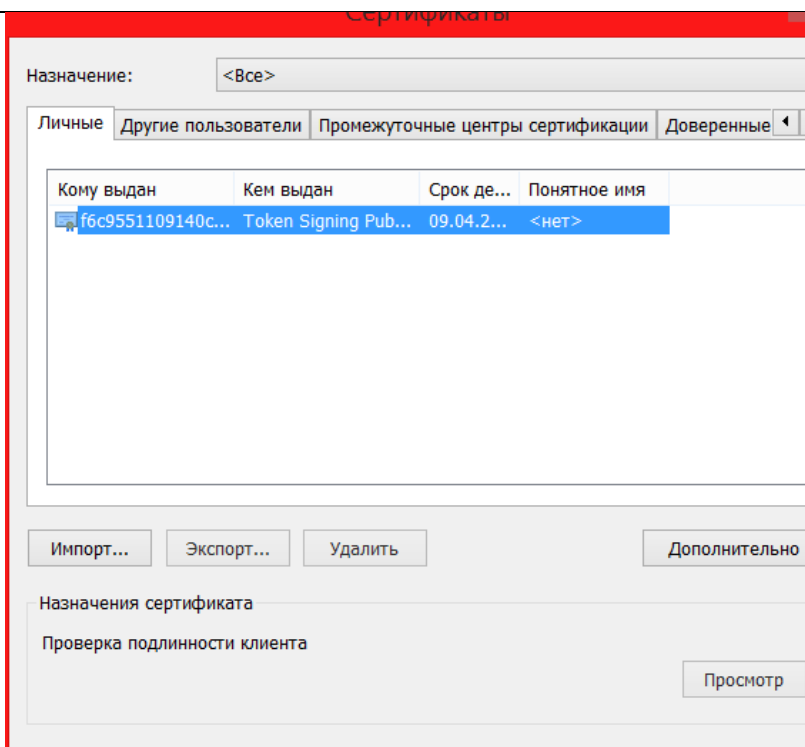
Отображение сайта с выключенными куки:

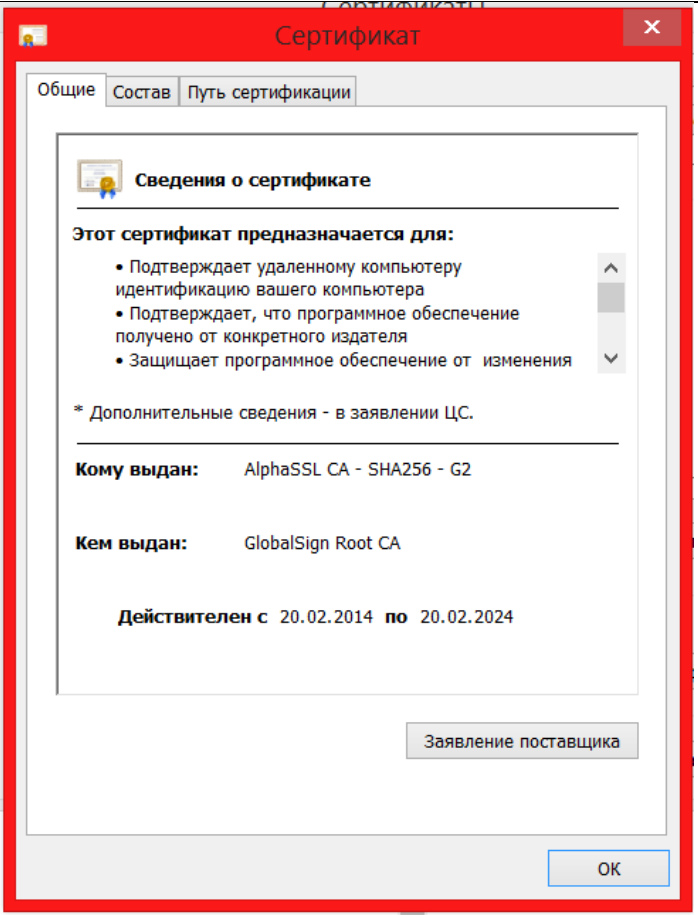
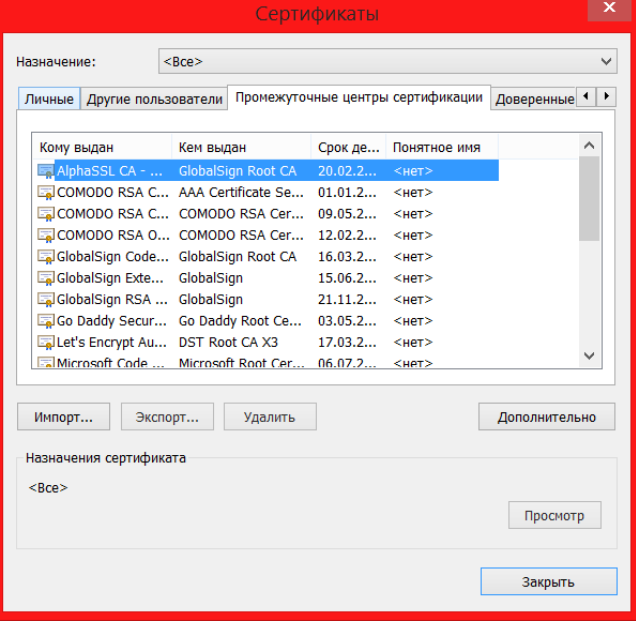
		<div data-bbox="994 94 1973 587"></div> <p>При отключении куки-файлов на сайте перестали отображаться его разделы, а также видеофон.</p>
3	Выполнить запрет на синхронизацию.	<div data-bbox="1187 660 1783 1270"></div>

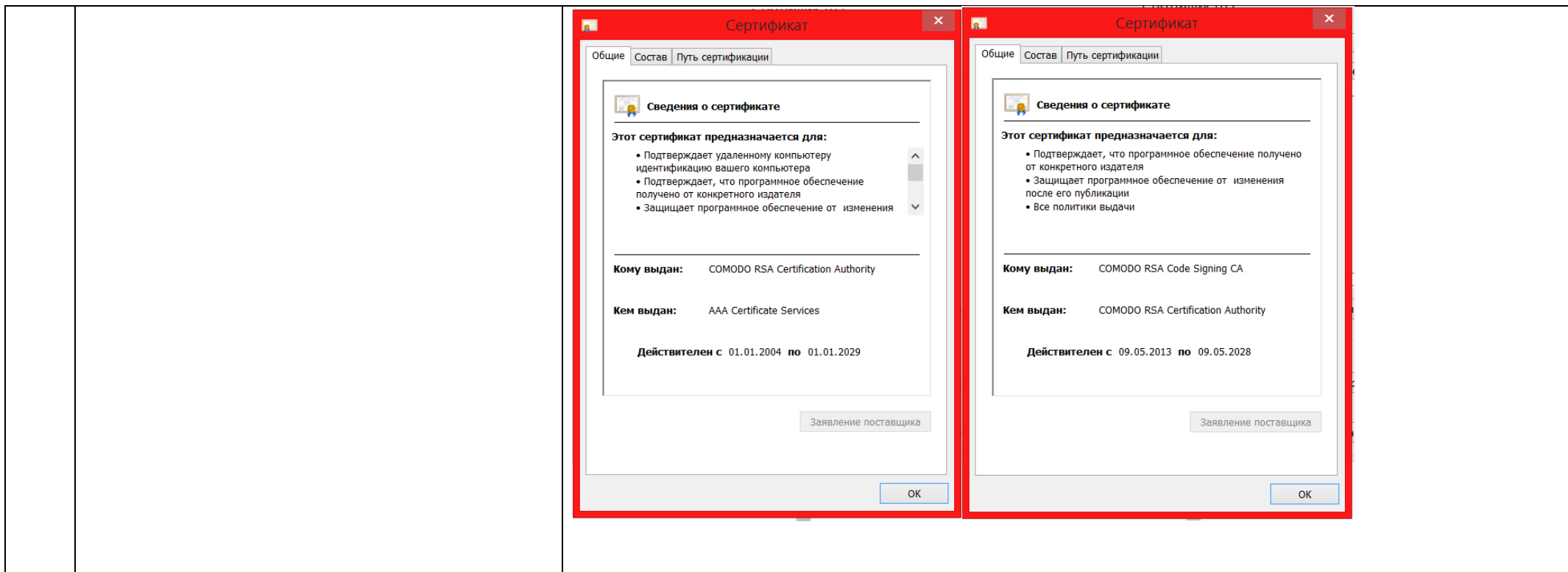
4	Включить режим инкогнито.	<div><div></div><div>Режим инкогнито</div><div><p>Ваши действия в режиме инкогнито будут недоступны другим пользователям этого устройства. Однако закладки, скачанные файлы и объекты из списка для чтения сохраняются. Подробнее</p><div><div><p>В Chrome не будет сохраняться следующая информация:</p><ul style="list-style-type: none">• история браузера;• файлы cookie и данные сайтов;• сведения, которые вы указываете в формах.</div><div><p>Ваши действия будут видны:</p><ul style="list-style-type: none">• сайтам, которые вы посещаете;• вашему системному администратору;• интернет-провайдеру.</div></div><div><div>Блокировать сторонние файлы cookie</div><div>Когда эта настройка включена, сайты не могут использовать файлы cookie, которые отслеживают ваши действия в Интернете. Из-за этого некоторые функции на сайтах могут работать некорректно.</div><div><input checked="" type="checkbox"/></div></div></div></div>
5	Вернуть начальные настройки браузера.	<div><div>Сбросить настройки?</div><div>Произойдут следующие изменения:</div><div><ul style="list-style-type: none">• сброс настроек и сочетаний клавиш в Chrome;• отключение расширений;• удаление файлов cookie и других временных данных сайтов.</div><div>Вам по-прежнему будут доступны закладки, история и сохраненные пароли. Подробнее</div><div><div>Отмена</div><div>Сбросить настройки</div></div><div><div><input checked="" type="checkbox"/></div><div>Отправьте отчет о текущих настройках Chrome, чтобы помочь нам улучшить браузер</div></div></div>

6

Проверить наличие цифровых сертификатов, описать назначение 2-3 цифровых сертификатов.







7. Контрольные вопросы:

- Всегда ли необходимо отключать файлы куки? Обоснуйте ответ.
Куки-относится к временным текстовым файлам. Там хранится информация персонального характера. Если куки отключены, то их придется снова включать при переходе на сайт, требующий поддержку куки. Поэтому нет необходимости отключать файлы куки, поскольку большинство сайтов требуют поддержку этих файлов. Достаточно просто регулярно производить очистку куки файлов, чтобы не сталкиваться с рядом различных проблем, в т.ч. ко взлому почтового ящика, копированию личных данных и т.д.
- В каких случаях необходимо включать режим инкогнито?
Режим инкогнито необходимо включать для дополнительного сохранения конфиденциальности, поэтому в браузерах, где включен этот режим истории и куки-файлы не будут сохраняться. Это удобный способ сохранить историю посещенных сайтов в секрете.

8. Выводы о проделанной работе. Благодаря данной практической работе я возобновила свои знания в сфере различных способов защиты данных в браузерах (поработала с куки-файлами, кэшем, режимом инкогнито и цифровыми сертификатами).

Практическое занятие № 2

1. Наименование практического занятия: Защита документов в MSOffice.
2. Цели практического занятия: Исследовать возможности настройки защиты документов в MSOffice.
3. Количество часов: 2
4. Место проведения: главный корпус РКСИ, ауд. 420.
5. Перечень используемого оборудования: компьютер, выход в глобальную сеть, комплект учебно-методической документации, раздаточный материал, операционная система MSWindows, MSOffice.
6. Последовательность проведения работ:

№ п/п	Этап выполнения задания	Описание выполняемых работ
1	<p>1. В текстовом редакторе MS Word в пункте меню <i>файл</i> → <i>сведения</i> → <i>защитить документ</i> реализовать следующие механизмы защиты:</p> <p>а. Установить пароль на открытие документа.</p> <p>б. Установить ограничение на редактирование «только чтение» для текущего документа.</p> <p>с. Определить произвольные фрагменты документа и группы пользователей, которым разрешено их редактирование.</p> <p>д. Установить защиту на редактирование.</p> <p>е. Пометить документ как окончательный.</p>	См. рис. 2.1-2.6
2	<p>1. В текстовом редакторе MS Excel в пункте меню <i>файл</i> → <i>сведения</i> → <i>защитить книгу</i> реализовать следующие механизмы защиты:</p>	См. рис. 3.1-3.6

	<p>а. Установить пароль на открытие документа.</p> <p>б. Установить защиту на все листы книги, разрешив только выделение ячеек.</p> <p>с. Выполнить защиту структуры книги.</p> <p>д. Пометить документ как окончательный.</p>	
--	--	--

Сведения

Yunasheva_Otchet_po_PZ_MDK_03_01

Рабочий стол



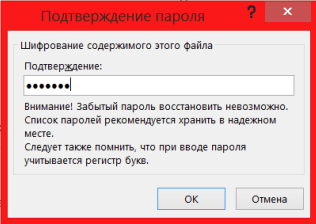
Режим ограниченной функциональности
Некоторые новые возможности отключены во избежание проблем при работе с предыдущими версиями Office. Преобразование этого файла позволит включить эти возможности, но может вызвать изменение разметки.

Свойства

Размер 7,8
Число страниц 59
Число слов 35!
Общее время правки 38;



Защита документа
Все могут открывать, копировать и изменять любую часть



Инспектор документов
Перед публикацией этого файла не забудьте, что он содержит:
■ Свойства документа, имя автора и обрезанные данные
■ Знаки, отформатированные как скрытый текст
■ Настраиваемые XML-данные
■ Содержимое, которое не смогут прочесть люди с ограниченными возможностями



Версии
Нет предыдущих версий этого файла.

Кем изменено

Связанные документы

Открыть расположение

Показать все свойства

Рис. 2.1

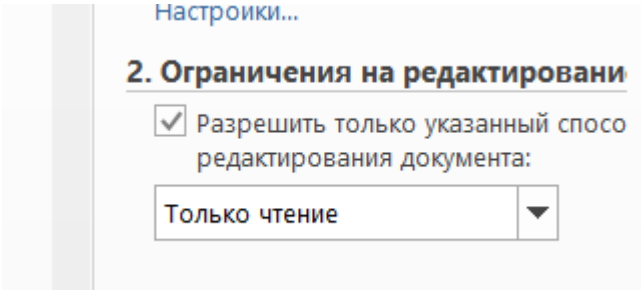


Рис. 2.2

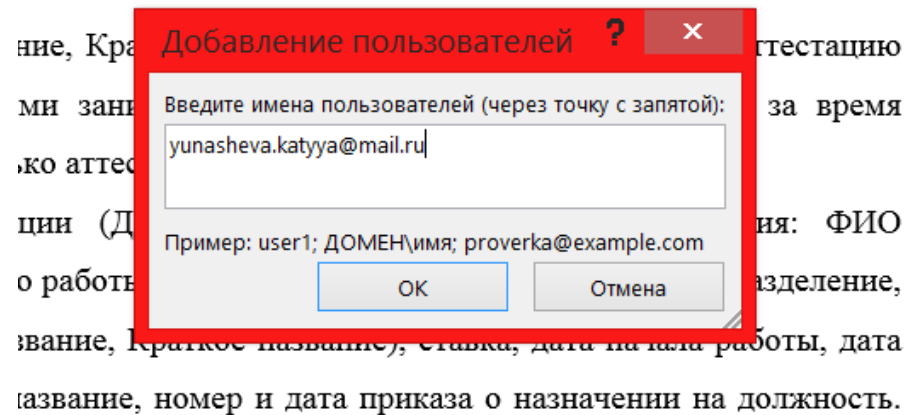


Рис. 2.3

предприятия».

Описание предметной области.

Предприятие (Код, Название, Краткое название) периодически проводит аттестацию сотрудников на соответствие ими занимаемой должности. Каждый сотрудник за время работы может проходить несколько аттестаций.

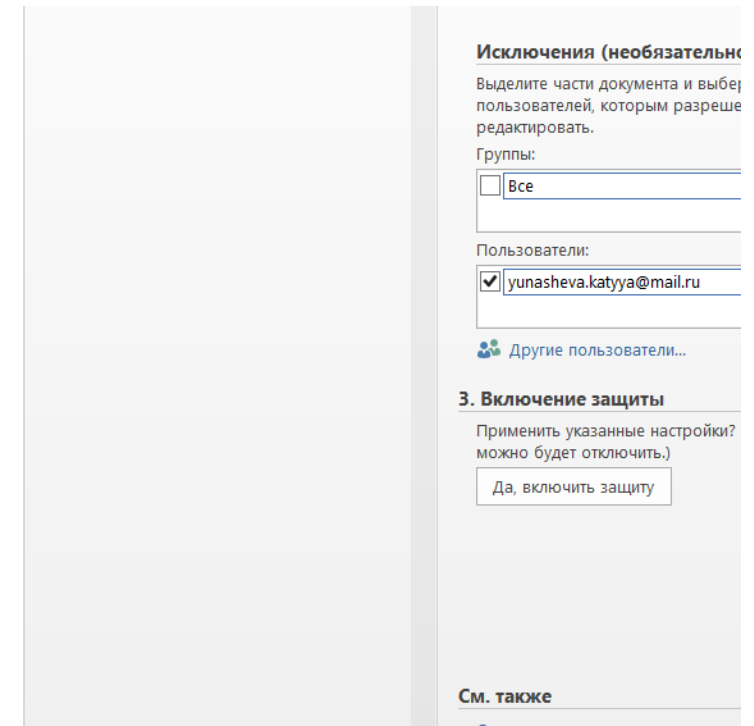
Для проведения аттестации (Дата) необходима следующая информация: ФИО сотрудника, дата рождения, место работы (Код, Название, Краткое название), подразделение, занимаемая должность (Код, Название, Краткое название), ставка, дата начала работы, дата окончания работы (контракта), название, номер и дата приказа о назначении на должность.

Необходимы также следующие сведения:

- сведения об образовании – какое заведение окончил, документ об образовании, квалификация по образованию (инженер, учитель, экономист);
- дата начала трудового стажа;
- дата начала стажа по специальности;
- сведения о повышении квалификации – в каком заведении проходил, дата начала, дата окончания прохождения.

У каждого сотрудника может быть несколько документов об образовании и

Рис. 2.4



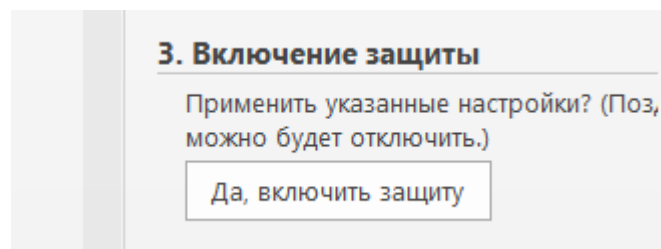


Рис. 2.5

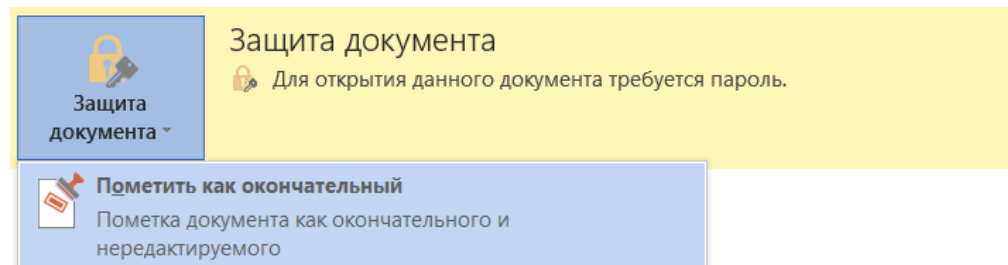


Рис. 2.6

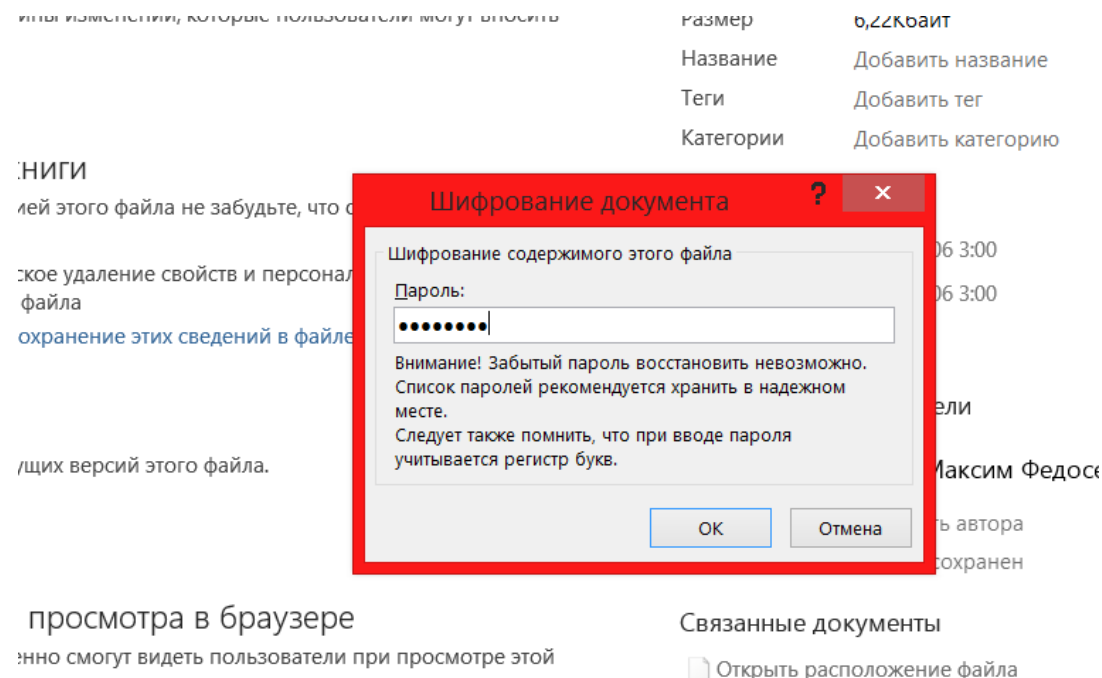


Рис. 3.1

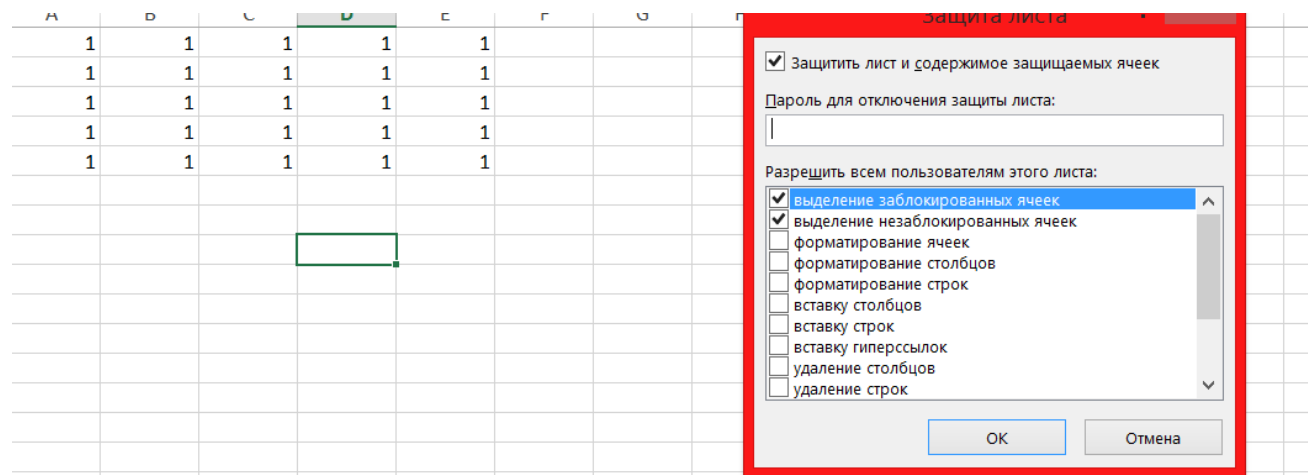


Рис. 3.2

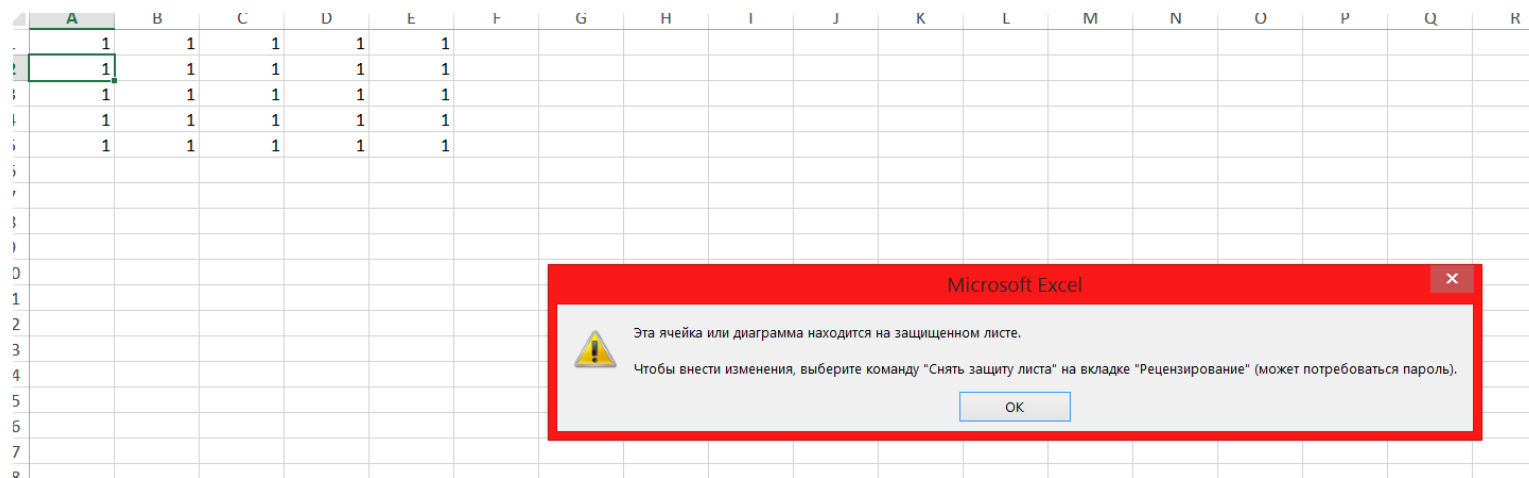


Рис. 3.3

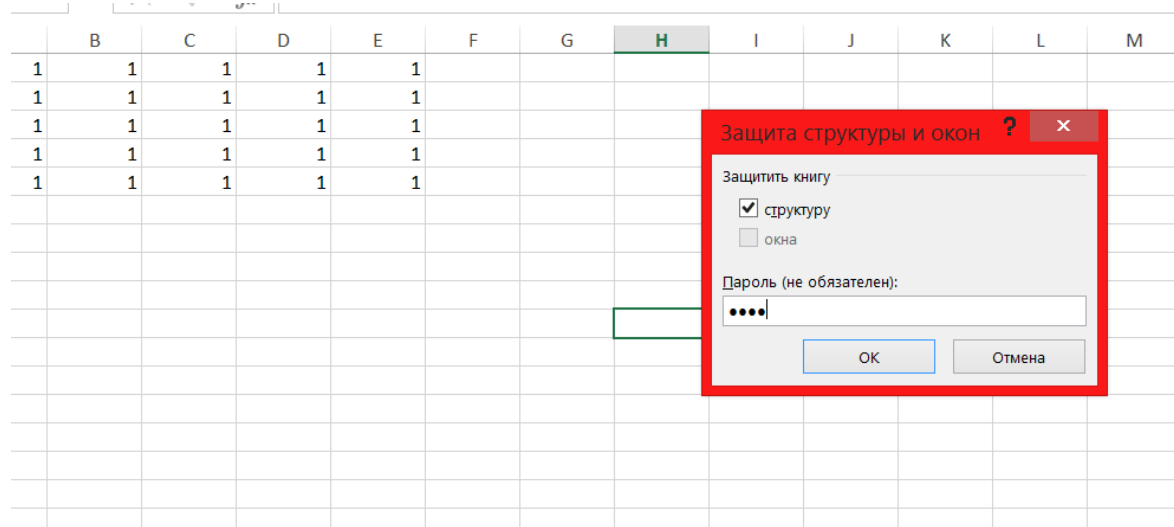


Рис. 3.4

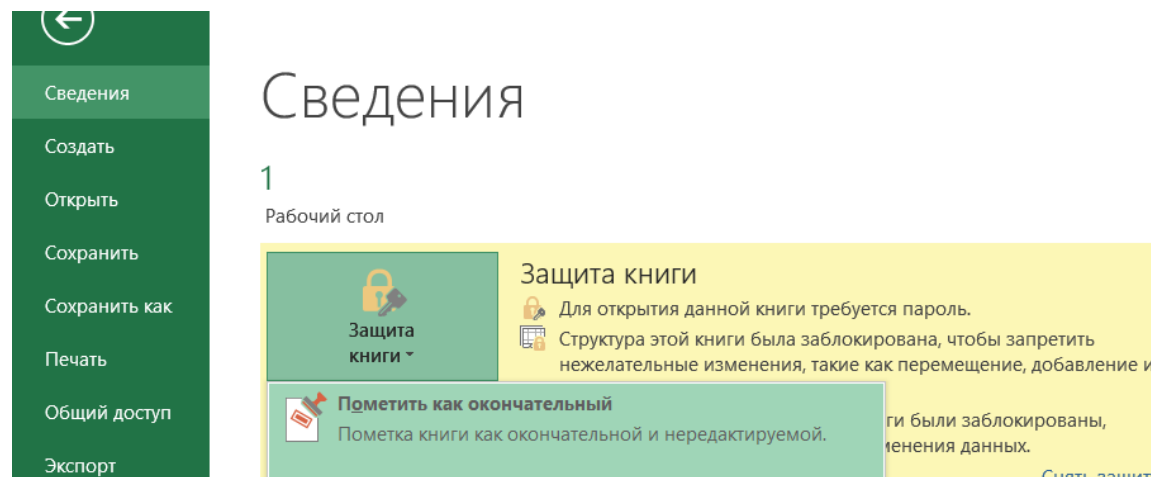


Рис. 3.5

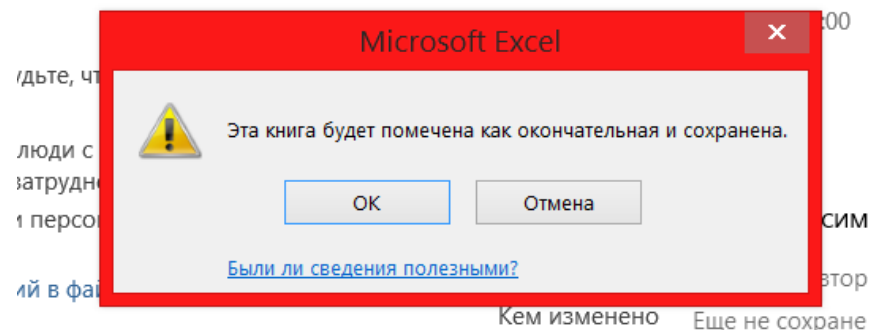


Рис. 3.6

7. Контрольные вопросы:

1. MS Word. Что подразумевается под опцией «окончательный документ»? Какие действия с ним возможны?
Если документ является «окончательным», то теперь запрещено любое редактирование, кроме копирования.
2. MS Word. Как снять пароль на документе?
Для того, чтобы снять пароль на документе, необходимо зайти в файл, далее защита документа, затем зашифровать с использованием пароля и очистить поле где мы вводили пароль, сохранить. После этого все смогут открывать, копировать и изменять любую часть документа.
3. MS Word. В каком случае опция «зашифровать паролем» будет доступна?
Опция «зашифровать паролем» будет доступна в любом случае, если документ не помечен как «окончательный».
4. MS Word. Как отменить защиту на редактирование областей документа?
Файл, защита документа, ограничить редактирование, убрать галочку «Разрешить только указанный тип редактирования».
5. MS Excel. Какие действия по защите книги необходимо выполнить, чтобы злоумышленник не нарушил ее структуру?
Файл, защита книги, защитить структуру книги.
6. MS Excel. Сможет ли защита элементов листа и книги не допустить компрометации книги? Обоснуйте ответ.
Защита листа не является функцией безопасности, потому что она только запрещает изменять заблокированные ячейки на данном листе. Для того, чтобы не допустить компрометацию книги, можно зашифровать сам файл паролем, чтобы другие пользователи не смогли открыть его.

8. Выводы о проделанной работе. Благодаря данной практической работе, я отработала и закрепила знания о возможности настройки защиты документов MS Word и MS Excel.

Практическое занятие № 3

1. Тема практического занятия: Программная реализация алгоритма шифрования и дешифрования информации.
2. Цели практического занятия: Создание программы, реализующей алгоритм шифрования и дешифрования информации.
3. Количество часов: 8
4. Место проведения: главный корпус РКСИ, ауд. 420.
5. Перечень используемого оборудования: компьютер, выход в глобальную сеть, комплект учебно-методической документации, раздаточный материал, операционная система MSWindows, среды программирования.
6. Последовательность проведения работ:

№ п/п	Этап выполнения задания	Описание выполняемых работ
1	Используя знания, умения и навыки, полученные при изучении дисциплины «Технология разработки программного продукта», распределить функции между членами группы, разработать постановку задачи, построить ее блок-схему.(Гончарова)	<p>Метод перестановки.</p> <p>При использовании шифров перестановки входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов. Перестановки в классической "докомпьютерной" криптографии получались в результате записи исходного текста и чтения шифрованного текста по разным путям геометрической фигуры.</p> <p>Простейшим примером перестановки является перестановка с фиксированным периодом d. В этом методе сообщение делится на блоки по d символов и в каждом блоке производится одна и та же перестановка. Правило, по которому производится перестановка, является ключом и может быть задано некоторой перестановкой первых d натуральных чисел. В результате сами буквы сообщения не изменяются, но передаются в другом порядке.</p> <p>В нашей работе мы будем делать одиночную перестановку по ключу. Столбцы таблицы с текстом переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.</p> <p>Для создания приложения были использованы HTML и JavaScript.</p> <p>Создана блок-схема алгоритма построения приложения.</p> <p>В ходе тестирования добавлен учет следующих ошибок:</p> <ol style="list-style-type: none">1) в ключе есть повтор букв;2) длина ключа должна составлять минимум 2 символа. См. Рис 1.

2	Используя любой язык программирования разработать программный продукт.(Куралин)	См. рис 2-4
3	Произвести его оптимизацию.(Юнашева)	Была проведена оптимизация программы.
4	Произвести отладку программы.(Гончарова)	Была проведена отладка программы.
5	Произвести тестирование программы.(Юнашева)	См. рис 5

Рис. 1

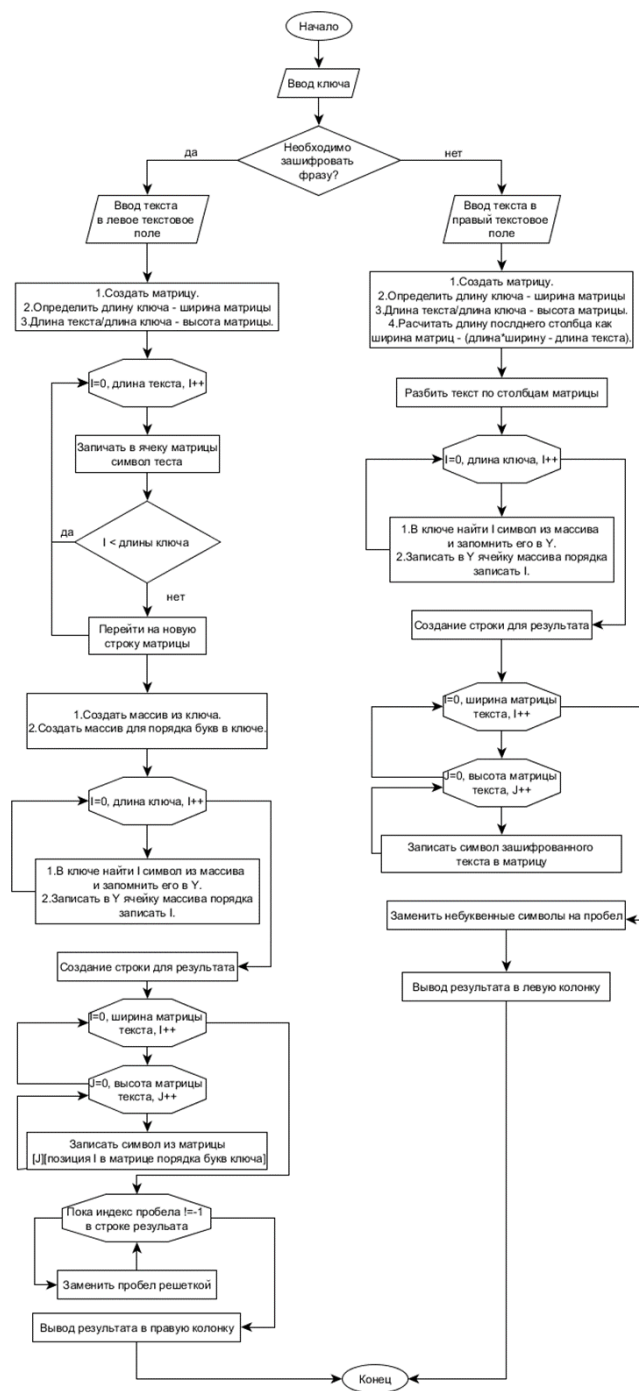


Рис. 2 Работа приложения:
Шифрование и дешифрование

Метод шифрования: Перестановка

Ключ:

Яблоки груши мандарины киви
вишни черешни

<=>

Ошибка: Ключ должен быть больше одного символа

Шифрование и дешифрование

Метод шифрования: Перестановка

Ключ:

Яблоки груши мандарины киви
вишни черешни

<=>

Ошибка: Символы в ключе не должны повторяться

Шифрование и дешифрование

Метод шифрования: Перестановка

Ключ:

Яблоки груши мандарины киви
вишни черешни

<=>

Яшннвшейлг#а##иекуаииичнб#идии
рормрkv##ш

Шифрование и дешифрование

Метод шифрования: Перестановка

Ключ:

Яблоки груши мандарины киви
вишни черешни

<=>

Яшннвшейлг#а##иекуаииичнб#идии
рормрkv##ш

Рис. 3 script.js:

```

1  let tb_key = document.getElementById('key');
2  let tb_input = document.getElementById('input_text');
3  let tb_output = document.getElementById('output_text');
4  let errorBlock = document.getElementById('error');
5
6  function error(text){
7      errorBlock.classList.toggle('_visible', Boolean(text));
8      errorBlock.innerHTML = text;
9  }
10 function validation(){
11     let word = tb_key.value
12     let isValid = true;
13     if(word.length > 1){
14         for (let i = 0; i < word.length; i++) {
15             let count = 0;
16             for (let j = 0; j < word.length; j++) {
17                 if(word[j] == word[i]) count++;
18             }
19             if(count != 1){
20                 isValid = false;
21                 error("<b>Ошибка:</b> Символы в ключе не должны повторяться");
22             }
23         }
24     }else{
25         isValid = false;
26         error("<b>Ошибка:</b> Ключ должен быть больше одного символа");
27     };
28     if(isValid) error(false);
29     return isValid;
30 }
31
32 function encode(text, key){
33     let matrix = [[]];
34     const width = key.length;
35     const height = Math.ceil(text.length / key.length);
36     let y = 0, x = 0;
37     for (let i = 0; i < text.length; i++) {
38         matrix[y][x] = text[i];
39         x++;
40         if(x > width-1 && i < text.length-1){
41             x = 0; y++;
42             matrix[y] = new Array();
43         }
44     }
45     let warr = key.split('').sort();
46     let chpos = [];
47     for (let i = 0; i < warr.length; i++) {
48         let pos = key.indexOf(warr[i]);
49         chpos[pos] = i;
50     }
51     let result = '';
52     for (let i = 0; i < width; i++) {
53         for (let j = 0; j < height; j++) {
54             result+= matrix[j]?.[chpos.indexOf(i)] || '';
55         }
56     }
57     while(result.indexOf(' ') != -1){result = result.replace(' ', '#')}
58     delete matrix;
59     return result;
60 }
61
62 function decode(text, key){
63     let matrix = [[]];
64     const width = key.length;
65     const height = Math.ceil(text.length / key.length);
66     const lats_line = width - (width * height - text.length);
67     for (let i = 0; i < height; i++){
68         matrix[i] = i < Math.floor(text.length / width) ? new Array(width)
69             : new Array(lats_line);
70     }
71     let warr = key.split('').sort();
72     let chpos = [];
73     for (let i = 0; i < warr.length; i++) {
74         let pos = key.indexOf(warr[i]);
75         chpos[pos] = i;
76     }
77     let index = 0;
78     for (let i = 0; i < width ; i++) {
79         for (let j = 0; j < height; j++) {
80             if( j*width + chpos.indexOf(i) < text.length ){
81                 matrix[j][chpos.indexOf(i)] = text[index];
82                 index++;
83             }
84         }
85     }
86     let result = '';
87     for (let i = 0; i < height; i++) {
88         for (let j = 0; j < width; j++) {
89             const ch = matrix[i]?.[j];
90             if(ch != undefined){
91                 result+= ch == '_' || ch == '#' || ch == ' ' ? ' ' : ch;
92             }
93         }
94     }
95     delete matrix;
96     return result;
97 }
98
99 function btn_encode(){
100     if(validation()){
101         tb_output.value = encode(tb_input.value, tb_key.value);
102     }
103 }
104
105 function btn_decode(){
106     if(validation()){
107         tb_input.value = decode(tb_output.value, tb_key.value);
108     }
109 }

```

Рис. 4 Основная разметка index.html:

```
1  <!DOCTYPE html>
2  <html lang="en">
3  <head>
4    <meta charset="UTF-8">
5    <meta http-equiv="X-UA-Compatible" content="IE=edge">
6    <meta name="viewport" content="width=device-width, initial-scale=1.0">
7    <link rel="stylesheet" href="style.css">
8    <title>Задание 3</title>
9  </head>
10 <body>
11   <div id="app">
12     <h2>Шифрование и дешифрование</h2>
13     <div style="font-size: 12px; color: gray; margin-bottom: 10px;">
14       Метод шифрования: Перестановка
15     </div>
16     <div class="key-box">
17       <label for="key">Ключ: </label><input id="key" type="text">
18     </div>
19     <table>
20       <tbody>
21         <tr>
22           <td><textarea id="input_text" cols="30" rows="10"></textarea></td>
23           <td>&lt;=&gt;</td>
24           <td><textarea id="output_text" cols="30" rows="10"></textarea></td>
25         </tr>
26         <tr>
27           <td colspan="3">
28             <div class="error" id="error" >Ошибка</div>
29           </td>
30         </tr>
31         <tr>
32           <td><button style="width: 100%;" onclick="btn_encode()">Зашифровать</button></td>
33           <td></td>
34           <td><button style="width: 100%;" onclick="btn_decode()">Дешифровать</button></td>
35         </tr>
36       </tbody>
37     </table>
38   </div>
39   <script src="script.js"></script>
```

Рис. 5 Тестирование программы:

Шифрование и дешифрование

Метод шифрования: Перестановка

Ключ:

Сообщение, которое ничего не значит

\Leftrightarrow

б,рчейсно#оноитн#аоеоинщ#ое#те
кегз

Зашифровать

Дешифровать

Шифрование и дешифрование

Метод шифрования: Перестановка

Ключ:

\Leftrightarrow

б,рчейсно#оноитн#аоеоинщ#ое#те
кегз

Зашифровать

Дешифровать

Шифрование и дешифрование

Метод шифрования: Перестановка

Ключ:

Сообщение, которое ничего не значит

\Leftrightarrow

б,рчейсно#оноитн#аоеоинщ#ое#те
кегз

Зашифровать

Дешифровать

Шифрование и дешифрование

Метод шифрования: Перестановка

Ключ:

где ты есть

\Leftrightarrow

#егтсдыте#ь

Зашифровать

Дешифровать

Шифрование и дешифрование

Метод шифрования: Перестановка

Ключ:

ныть

\Leftrightarrow

нъйт

Зашифровать

Дешифровать

Шифрование и дешифрование

Метод шифрования: Перестановка

Ключ:

пилотировать и упасть

\Leftrightarrow

ирьппитуюовисло#ата#т

Зашифровать

Дешифровать

7. Контрольные вопросы:

1. Какие языковые конструкции использованы в программе.

- Тернарный оператор, ceil, sort, split, indexOf, replace, floor.
- Использовались ли процедуры и функции? Описать их назначение.
Созданы функции error для всплывающего окна ошибки, validation для проверки правильности ключа, encode для шифрования, decode для дешифрования, btn_encode для запуска функции шифрования, btn_decode для запуска функции дешифрования.
 - Используя листинг программы, пояснить работу операторов выполняющих ключевые функции программы.

Пояснения:

```
function encode(text, key){  
  let matrix = [];  
  const width = key.length;  
  const height = Math.ceil(text.length / key.length);  
  let y = 0, x = 0;
```

Заполнение матрицы текстом, когда длина вставленного текста достигает длины ключа, то происходит переход к следующей строке матрицы:

```
  for (let i = 0; i < text.length; i++) {  
    matrix[y][x] = text[i];  
    x++;  
    if(x > width-1 && i < text.length-1){  
      x = 0; y++;  
      matrix[y] = new Array();  
    }  
  }  
  let warr = key.split("").sort();  
  let chpos = [];
```

1.В ключе найти I символ из массива и запомнить его в Y.

2.Записать в Y ячейку массива порядка записать I.

```
  for (let i = 0; i < warr.length; i++) {  
    let pos = key.indexOf(warr[i]);  
    chpos[pos] = i;  
  }
```

Записать символ из матрицы [J][позиция I в матрице порядка букв ключа]:

```
  let result = "";  
  for (let i = 0; i < width; i++) {
```

```

    for (let j = 0; j < height; j++) {
        result+= matrix[j]?.[chpos.indexOf(i)] || "";
    }
}

```

Замена пробелов:

```

while(result.indexOf(' ') != -1 ){result = result.replace(' ', '#')}
delete matrix;
return result;
}

```

```

function decode(text, key){
    let matrix = [[]];
    const width = key.length;
    const height = Math.ceil(text.length / key.length);
    const lats_line = width - (width * height - text.length);

```

Запись символов зашифрованного текста в матрицу:

```

    for (let i = 0; i < height; i++){
        matrix[i] = i < Math.floor(text.length / width) ? new Array(width) : new Array(lats_line);
    }
    let warr = key.split("").sort();
    let chpos = [];
    for (let i = 0; i < warr.length; i++) {
        let pos = key.indexOf(warr[i]);
        chpos[pos] = i;
    }

```

```

    let index = 0;
    for (let i = 0; i < width ; i++) {
        for (let j = 0; j < height; j++) {
            if( j*width + chpos.indexOf(i) < text.length ){
                matrix[j][chpos.indexOf(i)] = text[index];
                index++;
            }

```



```
    }  
  }  
}  
  
Создание результирующей строки:  
let result = "";  
for (let i = 0; i < height; i++) {  
  for (let j = 0; j < width; j++) {  
    const ch = matrix[i]?.[j];  
    if(ch !== undefined){  
      result+= ch == '_' || ch == '#' || ch == '' ? ' ': ch;  
    }  
  }  
}  
delete matrix;  
return result;  
}
```

8. Выводы о проделанной работе. Благодаря данной практической работе было разработано программа для шифрования и дешифрования текста методом перестановки с ключом.

Практическое занятие № 4

1. Наименование практического занятия: Система информационной безопасности в организации.
2. Цели практического занятия: Построить систему обеспечения информационной безопасности (СОИБ) условной организации, сформировать последовательность этапов построения СОИБ и перечислить мероприятия, реализуемые на каждом из этапов.
3. Количество часов: 8
4. Место проведения: главный корпус РКСИ, ауд. 420.

5. Перечень используемого оборудования: класс ПК, сеть Интернет, операционная система MS Windows, браузеры, MSOffice, индивидуальное задание, конспект лекций, комплект учебно-методической документации, электронные и бумажные методические и справочные материалы.
6. Последовательность проведения работ:

Ход занятия (деятельность студентов):

1. Организовать постоянный состав микрогруппы (ФИО участников заявить преподавателю).
2. Выбрать из предложенного списка организацию для реализации индивидуального задания.
3. Ознакомиться с электронными и бумажными методическими и справочными материалами.
4. Реализовать индивидуальное задание в соответствии с поставленными задачами.
5. Оформить полученные результаты в текстовом файле. Сдать на проверку преподавателю.

Список организаций (выбрать одну):

1. Салоны красоты.
2. Автомобили: прокат, аренда.
3. АЗС.
4. Выставки.
5. Строительное оборудование.
6. Кинотеатры.
7. Планетарий (дельфинарий).
8. Туризм.
9. Торговые базы.
10. Бытовые услуги.
11. Изготовление мебели.
12. Гостиница.
13. Издательские услуги.
14. Грузовые перевозки
15. Провайдеры.

Задачи (для любого индивидуального задания):

1. определить цели и задачи защиты информации в организации;
2. составить матрицу доступа;
3. определить группу требований к автоматизированной системе (АС);
4. определить предмет защиты в организации;

5. выявить возможные угрозы защищаемой информации в организации и их структуру;
6. выявить источники, виды и способы дестабилизирующего воздействия на защищаемую информацию в организации;
7. выявить каналы и методы несанкционированного доступа к защищаемой информации в организации;
8. определить основные направления, методы и средства защиты информации в организации.

При составлении файла необходимо придерживаться следующей структуры отчета:

1. Описание организации.
2. Характеристика информационной системы организации.
3. Актуальность проблемы защиты информации в организации.
4. Задачи индивидуального задания.
5. Цели и задачи защиты информации в организации.
6. Матрица доступа.
7. Требования по защите информации от НСД.
8. Объекты и предмет защиты в организации.
9. Угрозы защищаемой информации в организации.
10. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию в организации.
11. Каналы и методы несанкционированного доступа к защищаемой информации в организации.
12. Основные направления, методы и средства защиты информации в организации.
13. Выводы.

Критерии оценивания результатов практического занятия.

Результат	Критерии
Зачет	ставится, если студент выполнил работу в полном объеме с соблюдением необходимой последовательности действий; в ответе правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ ошибок. Работа студента характеризуется высокой и средней степенью самостоятельности. Отчет по практическому занятию сдан в установленные сроки.

Не зачет	ставится, если студент выполнил работу не полностью, объем выполненной части таков, что не позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки. Работа студента характеризуется низкой степенью самостоятельности. Отчет по практическому занятию не сдан в установленные сроки.
----------	---

7. Контрольные вопросы:

- *Какие нормативные документы использовались при построении СОИБ?*

Федеральным законом от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности»

Федерального закона от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании»

- *Является ли процедура построения СОИБ циклической? Обоснуйте Ваш ответ.*

Да, потому что это процесс, включающий осознание степени необходимости защиты информации и постановку задач; сбор и анализ данных о состоянии информационной безопасности в организации; оценку информационных рисков; планирование мер по обработке рисков; реализацию и внедрение соответствующих механизмов контроля, распределение ролей и ответственности, обучение и мотивацию персонала, оперативную работу по осуществлению защитных мероприятий; мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия.

- *Дайте характеристику современным злоумышленникам, совершающим правонарушения в сфере информационной безопасности.*

Современные злоумышленники чаще всего идут на получение информации незаконным путем для финансовой выгоды. Преступники реализуют множество других способов и инструментов для завладения чужими деньгами: используют дубликаты сим-карт потерпевших, а также устройства-скиммеры, считывающие информацию, содержащуюся на магнитной полосе банковской карты для последующего изготовления ее дубликата. Рассылают в социальных сетях со взломанных страниц пользователей сообщения их знакомым с просьбами одолжить деньги, внедряют вредоносные ПО в системы юридических лиц, похищают электронные ключи и учетные записи к нему в офисах организации и т.д.

- *Обоснуйте необходимость проведения регулярной работы с сотрудниками организации.*

Работа с персоналом по вопросам обеспечения информационной безопасности начинается в ходе процесса подбора и расстановки кадров, заканчивается – после увольнения сотрудника из организации.

Текущая работа с персоналом, обладающим конфиденциальной информацией, подразумевает:

- обучение и систематическое инструктирование работников;
- проведение регулярной воспитательной работы с персоналом, работающим с конфиденциальными сведениями и документами;
- постоянный контроль за выполнением персоналом требований по защите информации;
- аналитическую работу по изучению степени осведомленности персонала в области конфиденциальных работ;
- проведение служебных расследований по фактам утраты информации и нарушений персоналом требований по защите информации.

Процесс обучения работников правилам защиты информации должен быть систематическим и регулярным, т. к. состав и уровень ограничения доступа к конфиденциальной информации часто меняются, а система защиты, требует регулярного обновления и видоизменения.

- *Какова конечная цель полученной СОИБ?*

Конечной целью полученной СОИБ являются обеспечение защиты информации, внедрение и эксплуатация технических подсистем, комплексов и средств обеспечения информационной безопасности, обеспечение доступности соответствующих категорий информации для пользователей.

7. Выводы о проделанной работе. Благодаря данной практической работе была реализована система обеспечения безопасности МБОУ СОШ №1 ст. Тбилисской.

Индивидуальное задание:

1. Описание предприятия

МБОУ СОШ №1 ст.Тбилисская.

Пользователей – 60.

Компьютеров – 42.

Режим многопользовательский.

Есть выход в интернет.

Система распределенная.

Обрабатываемых данных больше 8 и меньше 500.

Нужно защитить персональные данные.

Школа включает в себя следующие отделы:

1. Совет администрации;
2. Педагогический совет;
3. Общешкольное собрание.

Уровни конфиденциальности:

1. персональные данные;
2. информация для служебного пользования.

В школе имеются следующие должности:

1. Директор;
2. Зам. директора по УВР;
3. Зам. Директора по ВР;
4. Системный администратор;
5. Главный бухгалтер;
6. Педагоги;
7. Психолог;
8. Охрана;
9. Заведующий хозяйством.

Характеристика информационной системы предприятия

Школа использует следующее программное обеспечение:

- пакет LibreOffice;
- OpenOffice;

Персональный компьютер есть у директора (анализирует работу школы, планирования деятельности и т.п.), у педагогов и психолога (для ведения учебной деятельности), у главного бухгалтера (рассчитывает заработную, расчеты с поставщиками, и прочие финансовые обороты школы), завхоз (ведет инвентаризацию и учет ведения склада), у охраны (для системы видеонаблюдения).

Системный администратор (администрирует школьный сервер).

Другие компьютеры персональными не являются и их используют другие работники в своих целях.

Для безопасного доступа пользователей локальной сети в Интернет, для защиты компьютеров от вторжений хакеров, вирусов, спама, точного подсчета трафика используется Интернет-шлюз SkyDNS на платформе Linux. В состав программного обеспечения входят прокси-сервер, межсетевой экран, антивирусная защита, система обнаружения атак, система анализа содержимого трафика, анти-спам.

Так как предприятие хранит персональные данные персонала и учеников, не подлежащие разглашению (т.е. доступ к которым разрешен не всем), в школе установлена система считывания индивидуальных электронных карт. Эти карты позволяют персоналу и школьникам зайти на территорию учебного заведения. Персональные данные видит только охрана. Такая система позволяет избежать использования личной информации и настроек данного школьника или персонала другим людям.

Так же для защиты помещений от несанкционированного доступа, в зданиях установлены камеры видеонаблюдения, система сигнализации, система противопожарной безопасности.

Актуальность проблемы защиты информации в школе

Обеспечение защиты информации в школе предусматривает необходимость защиты персональных данных. Наиболее важной представляется защита персональных данных, так как доверие сотрудников и учащихся в первую очередь основывается на предоставлении своих личных данных, и соответственно, сохранением их сотрудниками организации.

Поэтому целью обеспечения безопасности в школе является разработка политики безопасности и обеспечение надежной защиты информации на предприятии для его нормального функционирования.

Задачи

В данном задании практикантов поставлены следующие задачи:

1. определить цели и задачи защиты информации в школе;

2. составить матрицу доступа;
3. определить группу требований к автоматизированной системе (далее будет использовано сокращение АС);
4. определить предмет защиты на предприятии;
5. выявить возможные угрозы защищаемой информации в школе и их структуру;
6. выявить источники, виды и способы дестабилизирующего воздействия на защищаемую информацию в школе;
7. выявить каналы и методы несанкционированного доступа к защищаемой информации в школе;
8. определить основные направления, методы и средства защиты информации в школе.

2. Цели и задачи защиты информации в школе

Целями защиты информации школы являются:

- предупреждение хищения, утечки, утраты, искажения, подделки конфиденциальной информации (персональных данных);
- предотвращение угроз безопасности личности и учреждения;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию конфиденциальной информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в информационных системах;
- сохранение, конфиденциальности документированной информации в соответствии с законодательством.

К задачам защиты информации в учебном заведении относятся:

- обеспечение учебной деятельности школы режимным информационным обслуживанием, то есть снабжением всех служб, подразделений и должностных лиц необходимой информацией, как засекреченной, так и несекретной. При этом деятельность по защите информации по возможности не должна создавать больших помех и неудобств в решении производственных и прочих задач, и в то же время способствовать их эффективному решению, давать школе преимущества перед другими школами и оправдывать затраты средств на защиту информации.
- гарантия безопасности информации, ее средств, предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации;

- отработка механизмов оперативного реагирования на угрозы, использование юридических, экономических, организационных, социально-психологических, инженерно-технических средств и методов выявления и нейтрализации источников угроз безопасности учреждения;
- документирование процесса защиты информации, особенно сведений с тем, чтобы в случае возникновения необходимости обращения в правоохранительные органы, иметь соответствующие доказательства, что предприятие принимало необходимые меры к защите этих сведений;
- организация специального делопроизводства, исключающего несанкционированное получение конфиденциальной информации.

3. Матрица доступа

Основой политики безопасности является избирательное управление доступом, которое подразумевает, что все субъекты и объекты системы должны быть идентифицированы; права доступа субъекта к объекту системы определяются на основании некоторого правила (свойство избирательности).

Для описания свойств избирательного управления доступом применяется модель системы на основе матрицы доступа (МД), иногда ее называют матрицей контроля доступа. Матрица доступа представляет собой прямоугольную матрицу, в которой объекту системы соответствует строка, а субъекту столбец. На пересечении столбца и строки матрицы указывается тип разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту, как «доступ на чтение», «доступ на запись», «доступ на исполнение» и др.

Множество объектов и типов доступа к ним субъекта может изменяться в соответствии с некоторыми правилами, существующими в данной системе. Определение и изменение этих правил также является задачей МД.

Начальное состояние системы определяется матрицей доступа, все действия регламентированы и зафиксированы в данной матрице.

R – чтение из объекта;

W – запись в объект;

CR – создание объекта;

D – удаление объекта;

“+” – определяет права доступа для данного субъекта;

“–” – не определяет права доступа для данного субъекта.

Состояние системы считается безопасным, если в соответствии с политикой безопасности субъектам разрешены только определённые типы доступа к объектам (в том числе отсутствие доступа).

Объектами защиты в школе являются:

O1 – технические средства приема, передачи и обработки информации;

O2 – персональные данные школьников;
 O3 – персональные данные работников;
 O4 – документированная информация;
 O5 – личные дела работников;
 O6 – электронные базы данных работников и школьников;
 O7 – средства защиты информации (антивирусные программы, система сигнализации, система противопожарной охраны и др.);

Субъектами доступа к ресурсам школы являются:

S1 – Директор;
 S2 – Зам. директора по УВР;
 S3 – Зам. Директора по ВР;
 S4 – Системный администратор;
 S5 – Главный бухгалтер;
 S6 – Педагоги;
 S7 – Психолог;
 S8 – Охрана;
 S9 – Заведующий хозяйством.

Таблица 1. Матрица доступа

	O1	O2	O3	O4	O5	O6	O7	S6
S1	R, W	R, W, D, C R	R, W, D, C R	R, W, D, C R	R, W, D, C R	R, W, D, C R	R	+
S2	R	R, W	R	R	R	R	–	–
S3	R	R, W	R	R	R	R	–	–
S4	R, W, D C R	–	–	R	–	–	R, W, D C R	+

S5	-	-	R	R	R	R	-	-
S6	-	R, W	-	R	-	R	-	-
S7	R	R, W	R, W	R	R, W	R	-	-
S8	R, W	-	-	-	-	R	R, W	-
S9	R	-	-	R	-	-	-	-

4. Требования по защите информации от НСД

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД, условно состоящей из следующих четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

Формализованные требования к защите компьютерной информации АС.

Существует 3 группы АС с включающими в себя требованиями по защите систем. Но, учитывая структуру школы, рассматривается первая группа АС (в соответствии с используемой в классификацией), как включающую в себя наиболее распространенные многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности. Причем не все пользователи имеют право доступа ко всей информации АС.

5. Объекты и предметы защиты в школе

Основными объектами защиты в школе являются:

1. персонал (так как эти лица допущены к работе с охраняемой законом информацией (персональные данные) либо имеют доступ в помещения, где эта информация обрабатывается);

2. объекты информатизации – средства и системы информатизации, технические средства приема, передачи и обработки информации, помещения, в которых они установлены, а также помещения, предназначенные для проведения служебных совещаний;

3. информация ограниченного доступа, а именно:

- персональные данные работников (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, образование, профессия, уровень квалификации, доход, наличие судимостей и некоторая другая информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника);

- персональные данные школьников (фамилия, имя, отчество, дата рождения, телефон, данные о персональных документах, паспортные данные родителя (законного представителя));

4. защищаемая от утраты общедоступная информация:

- документированная информация, регламентирующая статус школы, права, обязанности и ответственность его работников (устав, журнал регистрации, учредительный договор, положение о деятельности, положения о структурных подразделениях, должностные инструкции работников);

- информация, которая может служить доказательным источником в случае возникновения конфликтных ситуаций (расписки);

5. материальные носители охраняемой законом информации (личные дела работников, личные дела школьников, электронные базы данных работников и школьников, бумажные носители и электронные варианты приказов, постановлений, планов, договоров, отчетов);

6. средства защиты информации (антивирусные программы, архиватор данных, программа для создания и восстановления резервной копии Linux, шифрование);

7. технологические отходы (мусор), образовавшиеся в результате обработки охраняемой законом информации (данные о бывших школьниках и сотрудников).

Предметом защиты информации в школе являются носители информации, на которых зафиксированы, отображены защищаемые сведения:

- база данных о школьниках и сотрудниках учебного заведения в бумажном и электронном виде;

- приказы, постановления, положения, инструкции, соглашения и обязательства о неразглашении, распоряжения, договоры, планы, отчеты, ведомость ознакомления с Положением о конфиденциальной информации и другие документы в бумажном и электронном виде.

6. Угрозы защищаемой информации в школе

Внешние угрозы:

- несанкционированный доступ к информации (хакеры, взломщики);

- вирусы;
- чрезвычайные ситуации;
- шпионские программы (флешки и т.п.);
- несанкционированное копирование;
- кража программно-аппаратных средств.

Внутренние угрозы:

- разглашение конфиденциальной информации сотрудниками школы;
- нарушение целостности данных со стороны персонала школы;
- потеря информации на жестких носителях;
- угрозы целостности баз данных;
- угрозы целостности программных механизмов работы школы;
- делегирование лишних или неиспользуемых полномочий на носитель с конфиденциальной информацией, открытие портов;
- системные сбои;
- повреждение аппаратуры, отказ программного или аппаратного обеспечения;
- угрозы технического характера;
- угрозы нетехнического или некомпьютерного характера – отсутствие паролей, конфиденциальная информация, связанная с информационными системами хранится на бумажных носителях.

7. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию

К источникам дестабилизирующего воздействия относятся:

- люди;
- технические средства отображения (фиксации), хранения, обработки, воспроизведения, передачи информации, средства связи и системы обеспечения их функционирования;
- природные явления.

Виды и способы дестабилизирующего воздействия на защищаемую информацию дифференцируются по источникам воздействия. Самое большее количество видов и способов дестабилизирующего воздействия имеет отношение к людям.

Со стороны людей возможны следующие виды воздействия, приводящие к уничтожению, искажению и блокированию:

- непосредственное воздействие на носители защищаемой информации;
- несанкционированное распространение конфиденциальной информации;

– вывод из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи;

– нарушение режима работы перечисленных средств и технологии обработки информации;

– вывод из строя и нарушение режима работы систем обеспечения функционирования названных средств.

Несанкционированное распространение конфиденциальной информации может осуществляться путем:

– словесной передачи (сообщения) информации;

– передачи копий (снимков) носителей информации;

– показа носителей информации;

– ввода информации в вычислительные сети;

– опубликования информации в открытой печати;

– использования информации в открытых публичных выступлениях, в т.ч. по радио, телевидению;

– потеря носителей информации.

Способами нарушения режима работы технических средств отображения, хранения, обработки, воспроизведения, передача информации, средств связи и технологии обработки информации, приводящими к уничтожению, искажению и блокированию информации, могут быть:

– повреждение отдельных элементов средств;

– нарушение правил эксплуатации средств;

– внесение изменений в порядок обработки информации;

– заражение программ обработки информации вредоносными программами;

– выдача неправильных программных команд;

– превышение расчетного числа запросов;

– передача ложных сигналов – подключение подавляющих фильтров в информационные цепи, цепи питания и заземления;

– нарушение (изменение) режима работы систем обеспечения функционирования средств.

К видам дестабилизирующего воздействия на защищаемую информацию со стороны технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи и систем обеспечения их функционирования относятся:

– выход средств из строя;

– сбои в работе средств

– создание электромагнитных излучений.

8. Каналы и методы несанкционированного доступа к защищаемой информации в школе

Для обеспечения защиты информации, содержащейся в информационной системе, оператором назначено структурное подразделение «Отдел защиты информации», ответственные за защиту информации.

Для проведения работ по защите информации в ходе создания и эксплуатации информационной системы обладателем информации (заказчиком) и оператором в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности»

Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании»

К числу наиболее вероятных каналов утечки информации можно отнести:

- визуальное наблюдение;
- подслушивание;
- техническое наблюдение;
- прямой опрос, выведывание;
- ознакомление с материалами, документами;
- сбор открытых документов и других источников информации;
- хищение документов и других источников информации;
- изучение множества источников информации, содержащих по частям необходимые сведения.

9. Организация комплексной системы защиты информации в школе

Для организации эффективной защиты конфиденциальной информации необходимо разработать программу, которая должна позволить достигать следующие цели:

- обеспечить обращение сведений в заданной сфере;
- предотвратить кражу и утечку конфиденциальной информации, любую порчу конфиденциальной информации;
- документировать процесс защиты данных, чтобы в случае попыток незаконного завладения какими-либо данными учреждения можно было защитить свои права юридически и наказать нарушителя.

Программа будет отражать размер данной школы, тип технологии и деловой информации, которую необходимо защищать.

В программе должны учитываться возможные источники и каналы утечки информации.

Для построения системы защиты конфиденциальной информации в школе необходимо создание службы защиты информации (далее – СлЗИ), которая будет являться структурной единицей школы, непосредственно участвующей в учебной деятельности. Работа этого отдела проводится во взаимодействии со структурными подразделениями учреждения. Структура и штат СлЗИ в зависимости от объема работ и особенностей учебной деятельности определяются руководителем учреждения и, как правило, должны комплектоваться инженерно-техническими работниками – специалистами основного профиля работы данной школы, а также специалистами, имеющими практический опыт защиты информации или работы с различными группами людей. Назначение на должность начальника СлЗИ школы, а также его освобождение производится только директором школы. Руководитель службы защиты информации регулярно, в установленные сроки отчитывается в своей работе перед директором школы.

Система доступа к конфиденциальным данным, должна обеспечить безусловное ознакомление с такими материалами только тех лиц, которым они нужны по службе. Система доступа к конфиденциальной информации – есть комплекс административно-правовых норм, обеспечивающих получение необходимой для работы информации каждым исполнителем и руководителем для экзаменационного процесса. Цель системы – обеспечить только санкционированное получение необходимого объема конфиденциальной информации. В структуру этой системы входят:

- разрешительная система доступа к документальной конфиденциальной информации;
- система пропусков и шифров, обеспечивающая только санкционированный доступ в помещения, где ведется экзаменационный процесс.

Для обеспечения физической сохранности носителей засекреченной информации и предотвращения доступа посторонних лиц нужна система охраны, которая включает в себя комплекс мероприятий, сил и средств, задействованных для предотвращения доступа посторонних лиц к носителям защищаемой информации.

Заключение

В процессе выполнения индивидуального задания практикантами была поставлена задача – создать и проанализировать средства информационной безопасности МБОУ СОШ №1 ст.Тбилисской. Поставленные цели были достигнуты при помощи классифицирования учреждения, были предложены методы и средства для усовершенствования политики безопасности данного учебного заведения, в результате выполнения которых школа позволит повысить эффективность средств защиты и сократит риск потери и искажения информации.

Следует обратить внимание на то, что только при совместном взаимодействии персонала, программно-аппаратных средств и средств защиты информации возможна эффективность данных мероприятий.

Данное учреждение циркулирует достаточно немалым количеством информации конфиденциального характера, доступ к которой необходимо ограничить. Поэтому, целью являлась разработка такой системы по защите информации, при которой угрозы утечки конфиденциальной информации были бы минимальны.

В результате анализа была построена модель информационной системы с позиции безопасности.

Никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в компьютерных сетях. В то же время свести риск потерь к минимуму возможно лишь при комплексном подходе к вопросам безопасности.