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 Линдаренко Милена Сергеевна

(Фамилия, имя, отчество)

Курс 4 Группа ПОКС-49

Общепрофессиональная дисциплина:
ОП.14 «Информационная безопасность»

Преподаватель колледжа:

_____ О.П. Манакова

Студент:

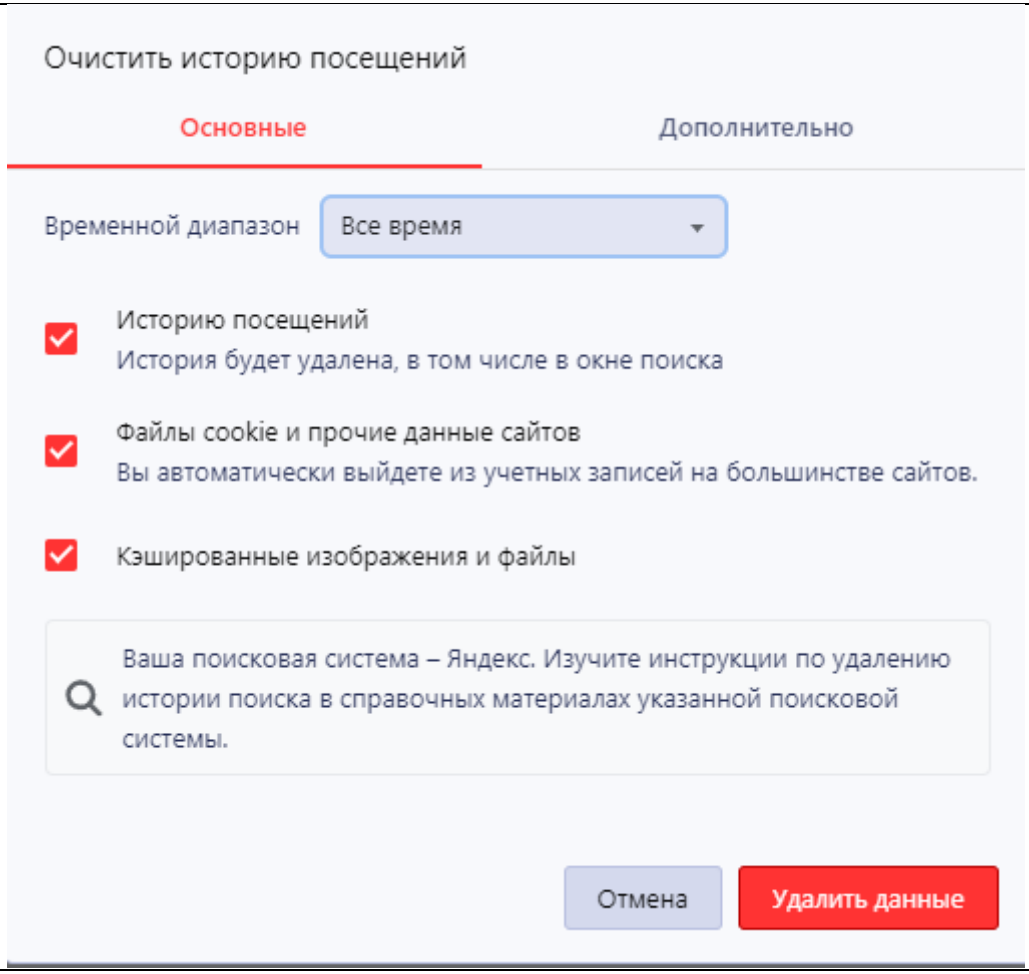
Линдаренко М.С.

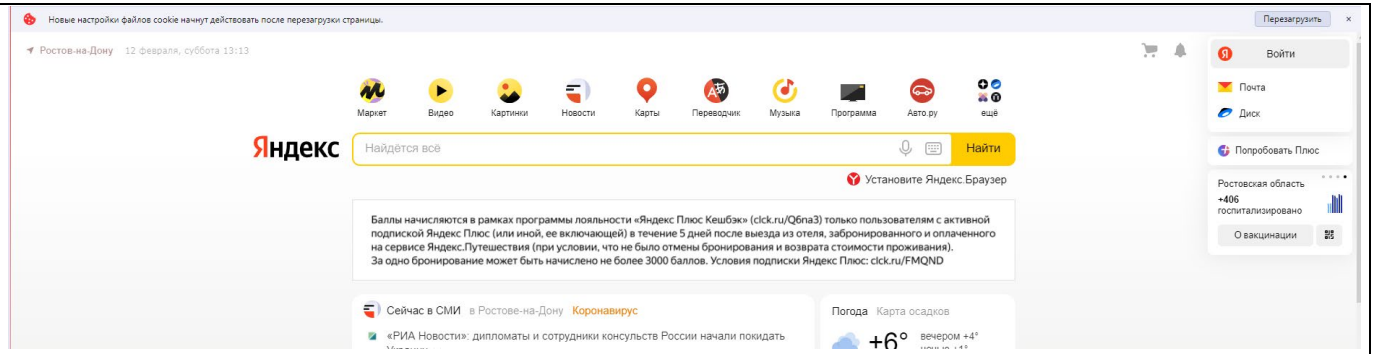
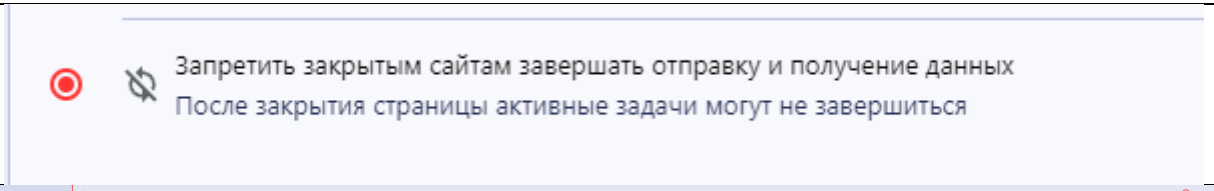
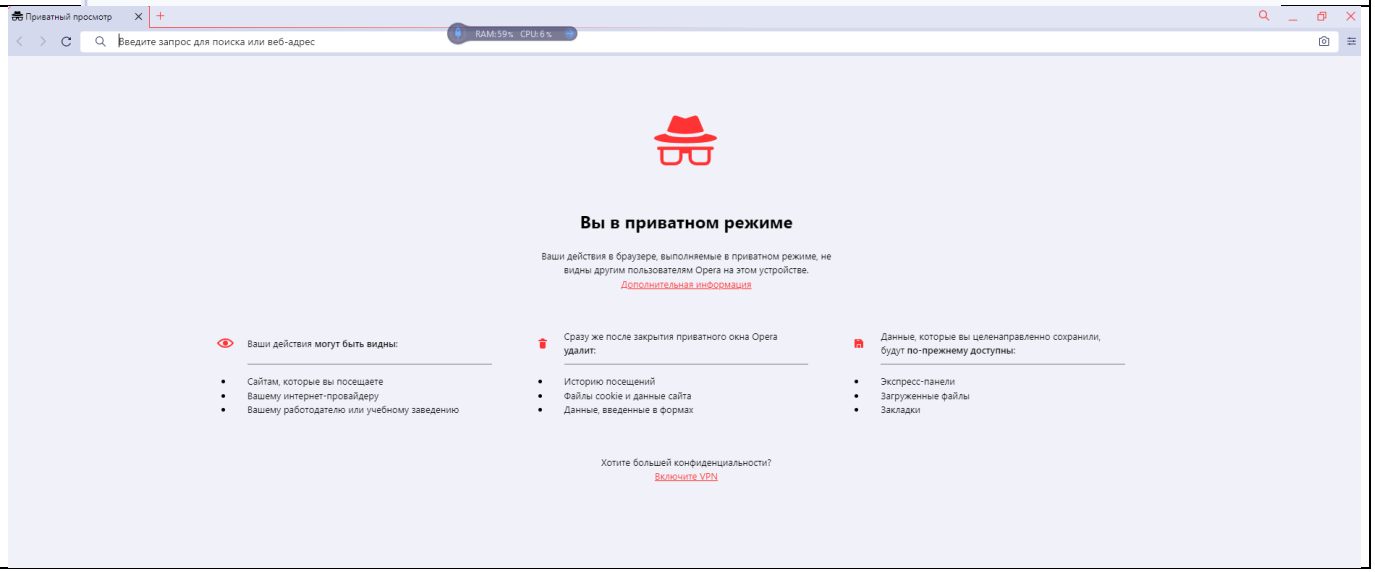
Ростов-на-Дону

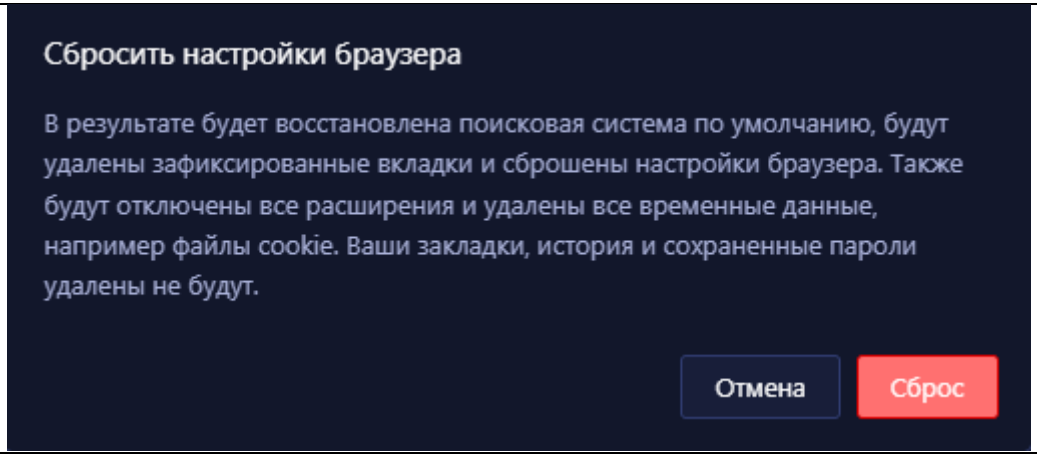
2021-2022 уч. г.

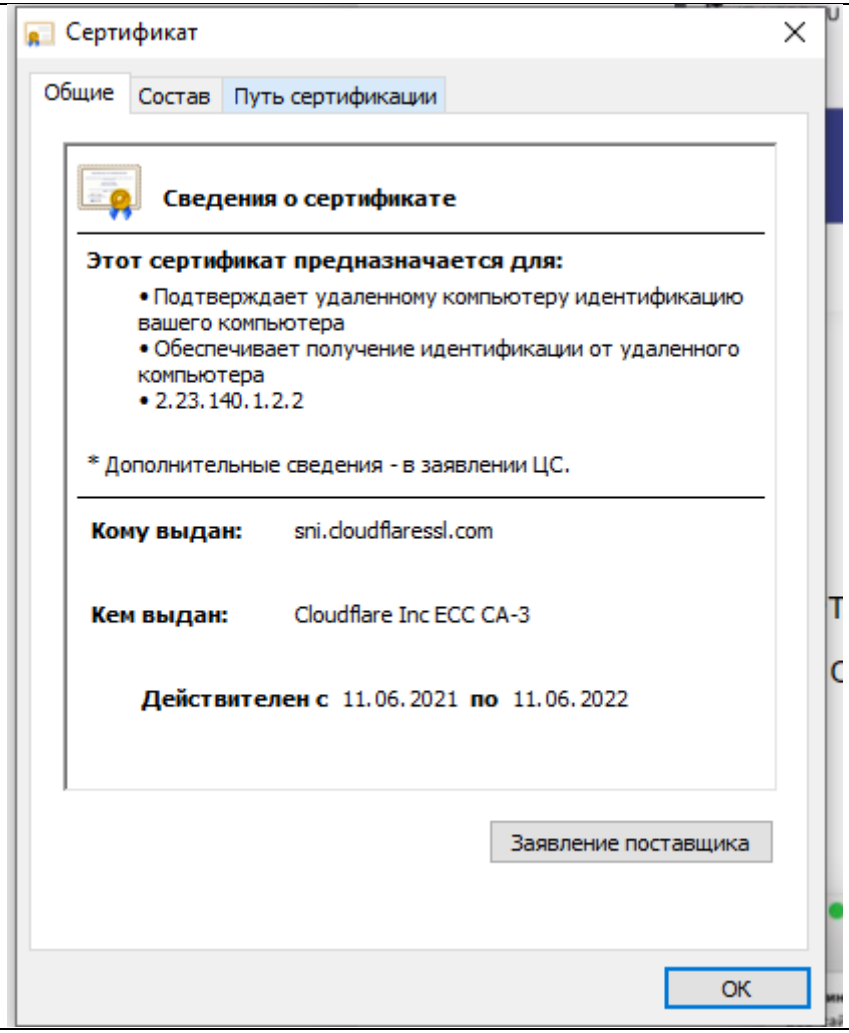
Практическое занятие №1

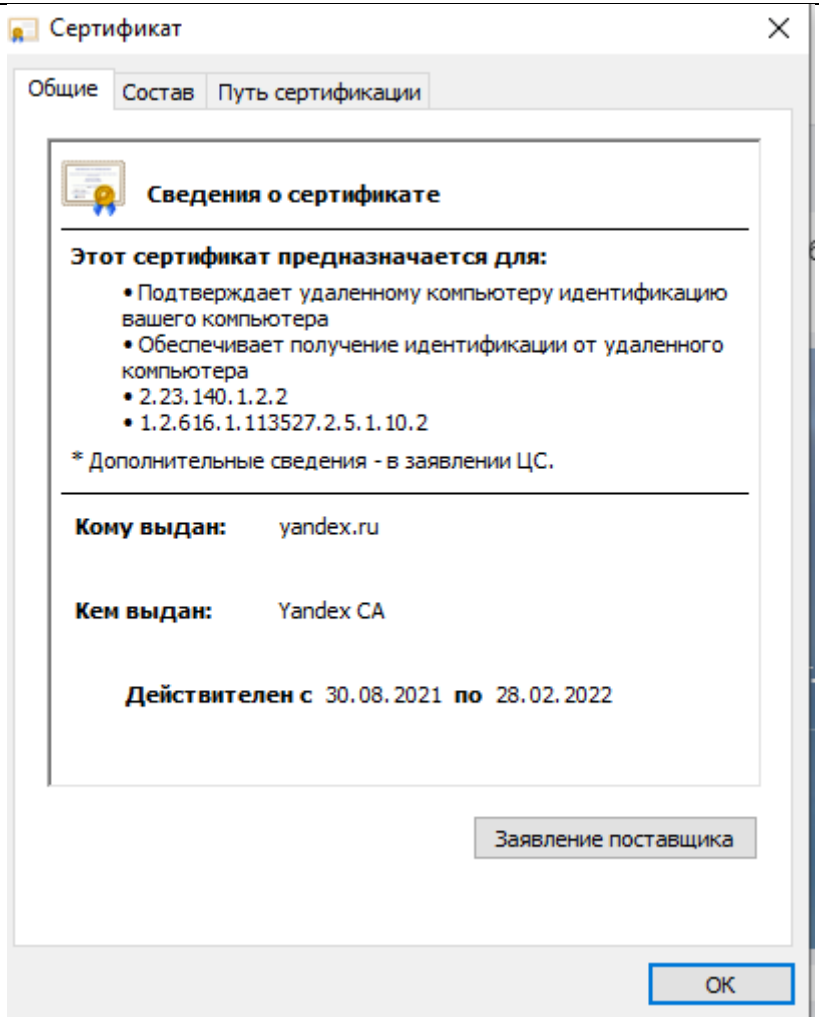
1. Наименование практического занятия: Настройки безопасности и конфиденциальности в браузере.
2. Цели практического занятия: Исследовать настройки безопасности и конфиденциальности в браузере.
3. Количество часов: 2
4. Место проведения: главный корпус РКСИ, ауд. 420.
5. Перечень используемого оборудования: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

№ п/п	Этап выполнения задания	Описание выполняемых работ
1	Очистить кэш и куки в браузере.	

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.).	
3	Выполнить запрет на синхронизацию.	
4	Включить режим инкогнито.	

5	Вернуть начальные настройки браузера.			

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



7. Контрольные вопросы:
   - Всегда ли необходимо отключать файлы куки? Обоснуйте ответ.
   - **По своей сути Cookies не несут никакого вреда для компьютера, они призваны облегчать вам работу в интернете. Они очень полезны и многие сайты, особенно интернет-магазины — используют их.**
     Но есть и небольшой риск, так, если кто-нибудь воспользуется вашим ПК с сохраненными куки, он сможет легко зайти в ваши аккаунты на сайтах.
   - В каких случаях необходимо включать режим инкогнито?
   - **Самый первый и самый частый случай это, когда вы находитесь не за своим компьютером и не хотите сохранять свои учетные данные на этом компьютере. Все, что нужно сделать, это открыть браузер в**

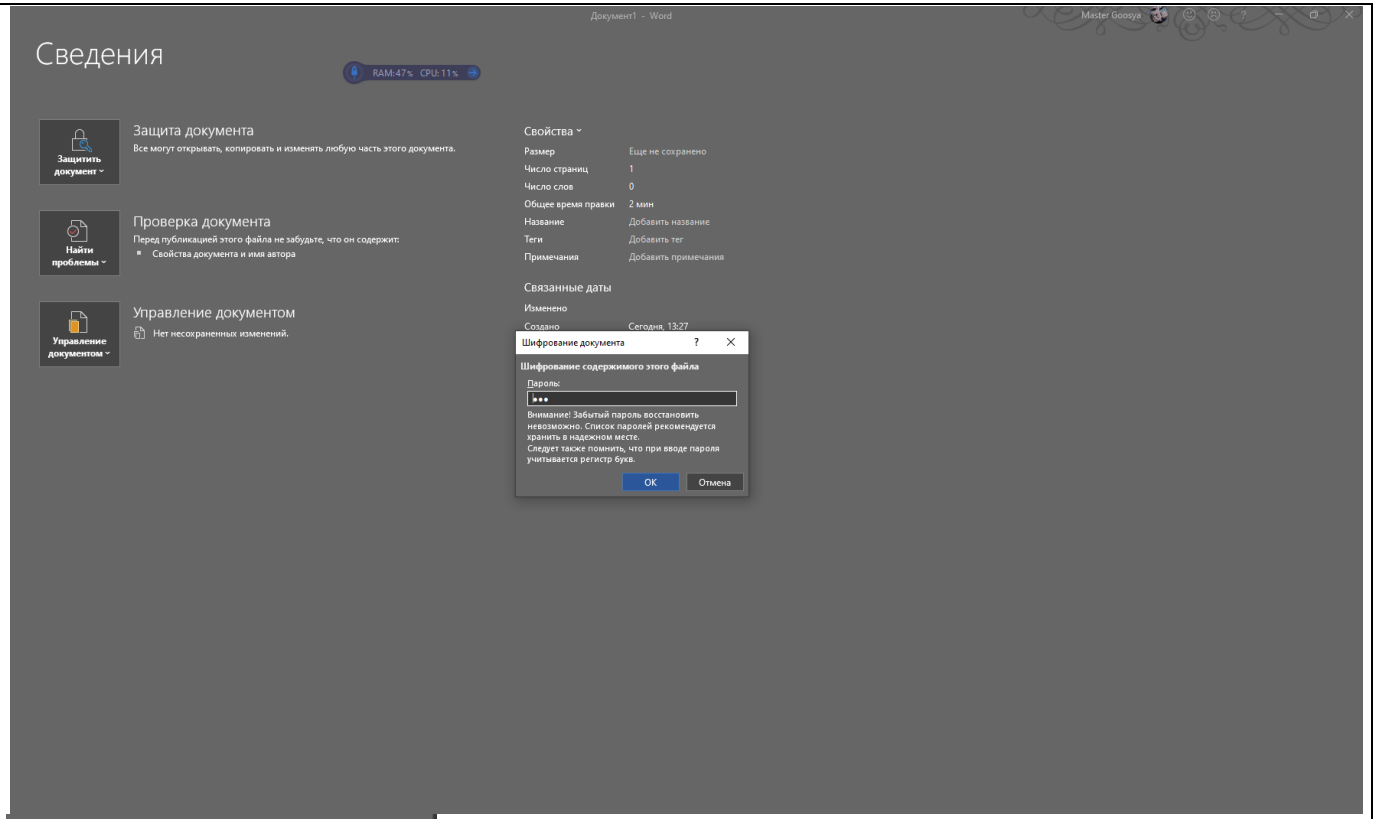
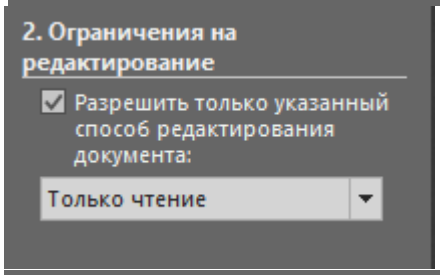
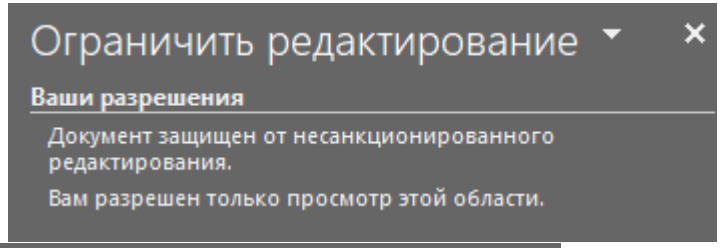
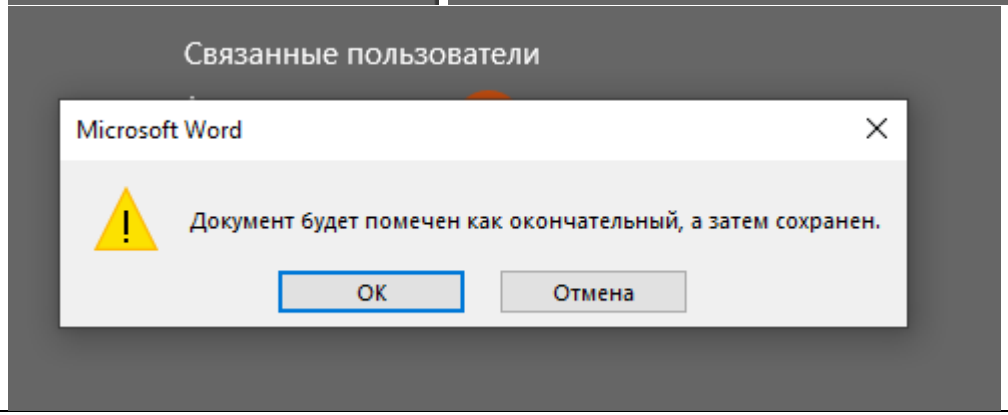
режиме инкогнито и использовать его. По окончанию работы мы просто закрываем окно и все введенные данные автоматически удалятся, за исключение скачанных файлов на сам компьютер.

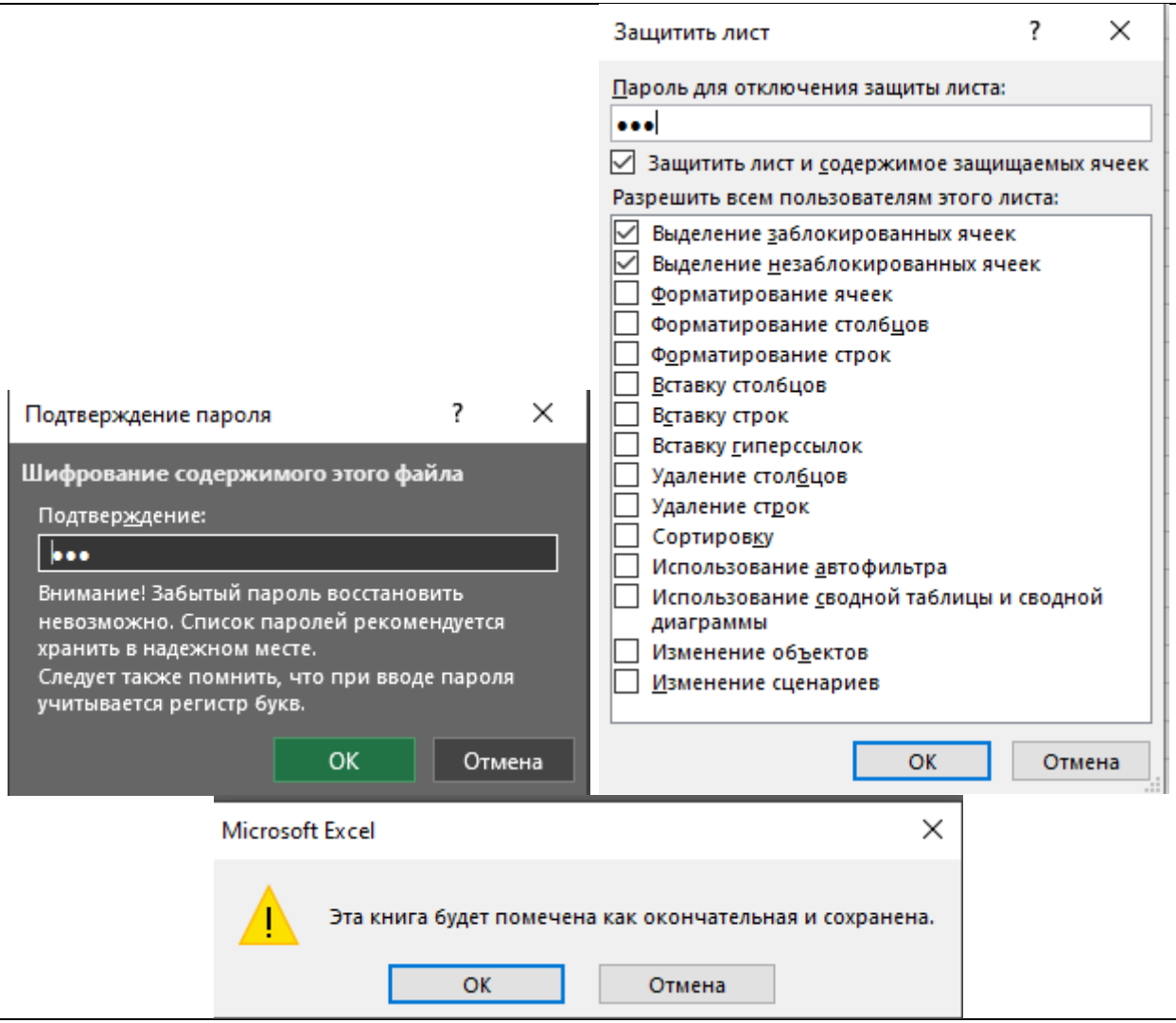
7. Выводы о проделанной работе.
   Я исследовала настройки безопасности и конфиденциальности в браузере, такие как cookie и кэш браузера, режим инкогнито и проверила наличие цифровых сертификатов у сайтов.

Практическое занятие № 2

1. Наименование практического занятия: Защита документов в MS Office.
2. Цели практического занятия: Исследовать возможности настройки защиты документов в MS Office.
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 MS Windows, MS Office.
6. Последовательность проведения работ:

№ п/п	Этап выполнения задания	Описание выполняемых работ

1	1. В текстовом редакторе MS Word в пункте меню *файл →сведения →защитить документ* реализовать следующие механизмы защиты: a. Установить пароль на открытие документа. b. Установить ограничение на редактирование «только чтение» для текущего документа. c. Определить произвольные фрагменты документа и группы пользователей, которым разрешено их редактирование. d. Установить защиту на редактирование. e. Пометить документ как окончательный.	   

2	1. В текстовом редакторе MS Excel в пункте меню *файл →сведения →защитить книгу* реализовать следующие механизмы защиты: a. Установить пароль на открытие документа. b. Установить защиту на все листы книги, разрешив только выделение ячеек. c. Выполнить защиту структуры книги. d. Пометить документ как окончательный.	

7. Контрольные вопросы:
   1. MS Word. Что подразумевается под опцией «окончательный документ»? Какие действия с ним возможны?
      С помощью пометки "Пометить как окончательный" можно сделать файл Word, Excel или PowerPoint файл только для чтения. Когда вы пометите файл как окончательный, команды ввода, редактирования, проверки оценок будут отключены или отключены, а файл станет доступно только для чтения, а для свойства Состояние документа будет установлено состояние Окончательный.
   2. MS Word. Как снять пароль на документе?

Откройте документ и введите пароль.
Перейдите в >файлов >защита > с помощью пароля.
Очистите поле Пароль и нажмите кнопку ОК.

3. MS Word. В каком случае опция «зашифровать паролем» будет доступна?
   Всегда, когда документ не помечен, как окончательный.
4. MS Word. Как отменить защиту на редактирование областей документа?
   Чтобы отключить защиту, следуйте приведенным ниже инструкциям: Убедитесь, что панель «Ограничить редактирование» открыта. Если вы его не видите, переключитесь на вкладку «Рецензирование» на ленте и нажмите «Ограничить редактирование» в разделе «Защита» на ленте.
5. MS Excel. Какие действия по защите книги необходимо выполнить, что бы злоумышленник не нарушил ее структуру? Установить защиту на все листы книги, разрешив только выделение ячеек.
   Выполнить защиту структуры книги.
   Пометить документ как окончательный.
6. MS Excel. Сможет ли защита элементов листа и книги не допустить компрометации книги? Обоснуйте ответ.
   Защита листа не является функцией безопасности. Она просто запрещает изменение заблокированных ячеек на листе.
   Защита листа отличается от защиты файла или книги Excel паролем. Дополнительные сведения см. ниже.

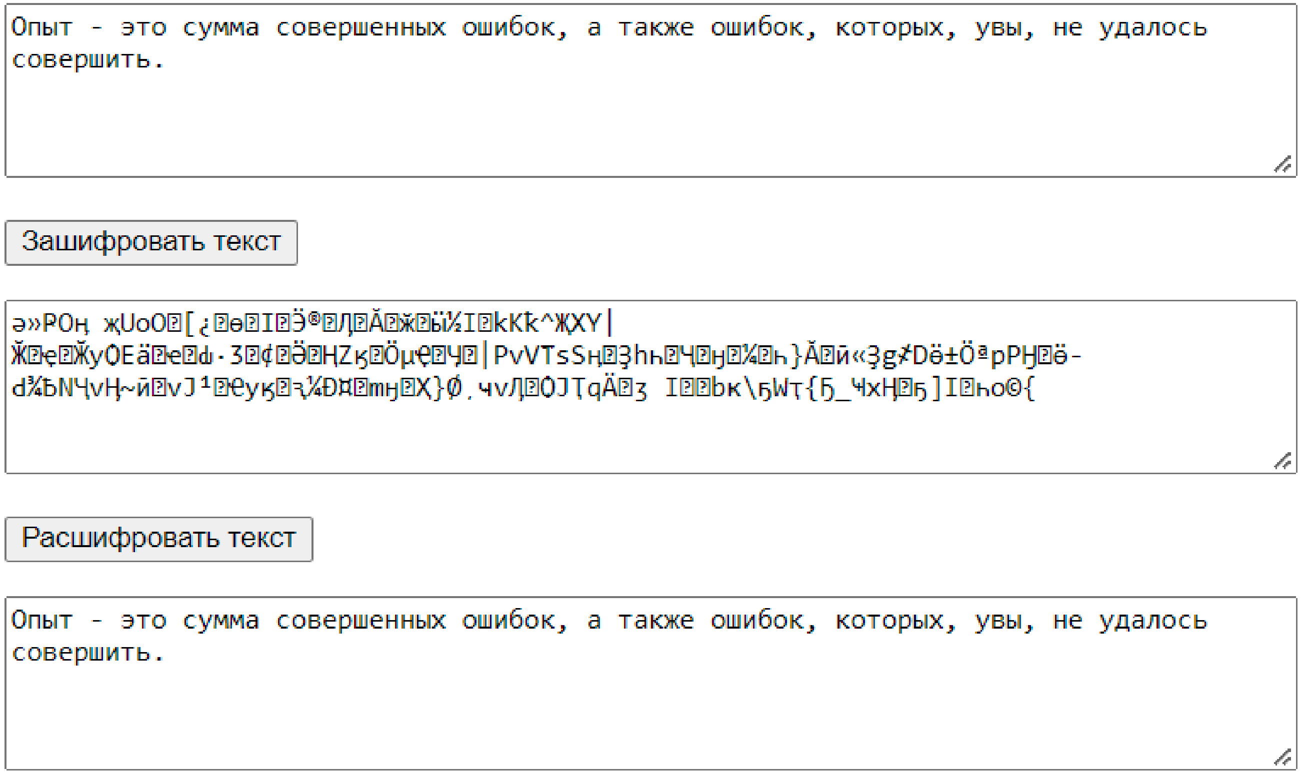
8. Выводы о проделанной работе.

В ходе выполнения практического задания были применены различные способы защиты документов Word и 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 MS Windows, 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.	Шифр подстановки — это метод шифрования, в котором элементы исходного открытого текста заменяются зашифрованным текстом в соответствии с некоторым правилом. Элементами текста могут быть отдельные символы (самый распространённый случай), пары букв, тройки букв, комбинирование этих случаев и так далее. Символы исходного текста кодируются и декодируются с помощью методов fromCharCode() и charCodeAt(). Каждый символ строки заменяется символом Unicode, код которого составляется из суммы кода исходного символа и случайного числа.
2	Используя любой язык программирования разработать программный продукт.	Для разработки были спользованы JavaScript и HTML.

3	Произвести тестирование программы.	

7. Контрольные вопросы:

1. Какие языковые конструкции использованы в программе. Length, random, round, charCodeAt(), fromCharCode().
2. Использовались ли процедуры и функции? Описать их назначение. Были использованы функции Encrypt() и unEncrypt() предназначенные для шифрования и дешифрования символьных строк.
3. Используя листинг программы, пояснить работу операторов выполняющих ключевые функции программы.
4.

```
function Encrypt(theText) {
output = new String;
Temp = new Array();
Temp2 = new Array();
TextSize = theText.length; //определяем длину введённой строки
for (i = 0; i < TextSize; i++) { //перебор символов строки
rnd = Math.round(Math.random() * 122) + 68; //генерация случайного числа
Temp[i] = theText.charCodeAt(i) + rnd; //присваиваем элементу первого массива значение, складывающееся из суммы кода символа (Unicode) и случайного числа
Temp2[i] = rnd; //элемент второго массива присваиваем значение случайного числа
}
for (i = 0; i < TextSize; i++) {// формирование результирующей строки
output += String.fromCharCode(Temp[i], Temp2[i]); // формируем строку путём преобразования значений элементов массивов в символы
```

```
16. }
17. return output; // возвращаем результирующую строку
18. }
```

8. Выводы о проделанной работе. **В ходе выполнения практического задания был создан программный продукт, предназначенный для шифрования и дешифрования символьных строк, с использованием JS и HTML.**

Практическое занятие № 4

1 Описание организации

ПАО «Альфа»

В качестве основного вида деятельности: Торговля розничная моторным топливом в специализированных магазинах.

Эта группировка включает:

- розничную торговлю топливом для автомобилей и мотоциклов в специализированных магазинах;
- розничную торговлю смазочными материалами и охлаждающими жидкостями для автотранспортных средств.

Автомобильная заправочная станция (АЗС) — это оборудованный комплекс, расположенный на придорожной территории. Основное ее предназначение — заправка топливом транспортных средств. Автозаправочная станция не ограничивается продажей только топлива, а работает как целостный комплекс по предоставлению всех необходимых и сопутствующих товаров и услуг. На территории АЗС находится место для небольшого магазина, банкомата, терминала для оплаты услуг, закусочной или кафе.

Компьютеров — 3

Пользователей — 3

Общее количество персонала — 6

Есть выход в интернет

Существует необходимость в защите персональных данных

Уровни конфиденциальности:

- конфиденциальные данные;
- информация для служебного пользования.

В организации имеются следующие должности:

- директор;
- старший кассир;
- кассир;
- автозаправщик;
- охранник.

2 Характеристика информационной системы организации

В организации используется следующее программное обеспечение:

- программный продукт «СНК-АЗС»;
- пакет Microsoft Office;
- платёжная система Orangepay;
- программный продукт «Компас» для управления персоналом.

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

Так же для защиты помещений от несанкционированного доступа, в кабинетах и проходных установлены камеры видеонаблюдения, система сигнализации, система противопожарной безопасности, радиочастотная противокражная система.

3 Актуальность проблемы защиты информации в организации

В России работает несколько десятков тысяч АЗС, лишь в Московской области их более 2000. А поскольку многие из этих комплексов оперируют в течение суток существенными суммами наличных денег, они всегда будут оставаться целью для тех, чьи действия подпадают под статью 162 УК РФ (разбой). Данные статистики говорят сами за себя. Доходит до того, что некоторые заправки подвергаются вооруженным нападениям многократно в течение относительно коротких промежутков времени. Многие топливные компании, занимающиеся розничной реализацией топлива, уже взяли за правило тренировать своих сотрудников путем проведения учебных нападений на АЗС. Обычно все учения начинаются с того, что сотрудник нажимает кнопку вызова подразделения оперативного реагирования, которое при соответствующей выучке прибудет на место минуты за три.

Проблему обеспечения безопасности можно условно разделить, как и на большинстве объектов, где есть торговые комплексы, на две части: защиту от внешних угроз (вооруженные нападения с целью грабежа, клиенты уезжают, не заплатив за топливо) и от внутренних (кражи товаров, денег и топлива недобросовестными сотрудниками самих АЗС). Методов кражи, которые использует персонал, существует великое множество. Некоторые топливные компании отказываются от схемы работы по "постоплате", стараясь тем самым минимизировать внешние риски, но это создает неудобства для клиента, так как вы не можете залить полный бак, например оплатив топливо пластиковой картой.

Еще один аспект обеспечения безопасности автозаправки связан с тем, что она является объектом повышенной пожарной и взрывоопасности. Необходимо постоянно иметь возможность разбирать различные спорные ситуации, связанные с автотранспортом клиентов, отслеживать процедуру слива нефтепродуктов из автоцистерн и в случае повреждения топливораздаточных колонок незамедлительно реагировать.

4 Задачи индивидуального задания

1 определить цели и задачи защиты информации на предприятии;
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 на предприятии и их структуру;
6 выявить источники, виды и способы дестабилизирующего воздействия на защищаемую информацию на предприятии;
7 выявить каналы и методы несанкционированного доступа к защищаемой информации на предприятии;
8 определить основные направления, методы и средства защиты информации на предприятии.

5 Цели и задачи защиты информации в организации

1 обеспечение сохранности денежных средств и товарно-материальных ценностей;
2 охрана сотрудников АЗС и ее клиентов;
3 ограничение доступа в помещения АЗС и (по необходимости) на прилегающую территорию;
4 выявление нарушений в режиме полноценной работы объекта (возгорание, неработоспособность оборудования, проникновение и т.д.);
5 предупреждение противозаконных действий со стороны персонала и сторонних лиц;
6 обеспечение контроля над соблюдением мер безопасности, правилами выполнения технологических операций и торговли;
7 оповещение персонала и клиентов АЗС о нештатных ситуациях;

8 взаимодействие с государственными правоохранительными органами по вопросам безопасности.

6 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 на предприятии являются:

O1 – технические средства приема, передачи и обработки информации;

O2 – данные клиентов;

O3 – персональные данные работников;

O4 – документированная информация;

O5 – личные дела работников;

O6 – средства защиты информации (антивирусные программы, система сигнализации, система противопожарной охраны и др.);

Субъектами доступа к ресурсам предприятия являются:

S1 – директор;

S2 – старший кассир;
S3 – кассир;
S4 – автозаправщики;

S5 – охранник; O1	O2	O3	O4	O5	O6
S1	R, W, CR, D	R, W, CR, D	R, W, CR, D	R, W, CR, D	R, W, CR, D	R, W, CR, D
S2	R	R, W,CR	-	R, W	-	R
S3	R	R	-	R	-	-
S4	-	-	-	-	-	-
S5	-	-	-	-	-	R, W, CR

Возможные варианты получения незаконного доступа:

- подключение к системам связи (телефонные линии, интеркомы, проводные переговорные устройства);
- хищение документации, в том числе ее копирование (тиражирование) с враждебными целями;
- непосредственное использование компьютеров, внешних накопителей или иных устройств, содержащих информацию;
- внедрение в операционную систему через Интернет, в том числе с использованием шпионских программ, вирусов и прочего вредоносного программного обеспечения;
- использование сотрудников компании (инсайдеров) в качестве источников сведений.

Методы защиты компьютеров от несанкционированного доступа делятся на программно-аппаратные и технические. Первые отсекают неавторизованных пользователей, вторые предназначены для исключения физического проникновения посторонних людей в помещения компании.

Создавая систему защиты информации (СЗИ) в организации, следует учитывать, насколько велика ценность внутренних данных в глазах злоумышленников.

Для грамотной защиты от несанкционированного доступа важно сделать следующее:

- отсортировать и разбить информацию на классы, определить уровни допуска к данным для пользователей;

- оценить возможности передачи информации между пользователями (установить связь сотрудников друг с другом).

В результате этих мероприятий появляется определенная иерархия информации в компании. Это дает возможность разграничения доступа к сведениям для сотрудников в зависимости от рода их деятельности.

Аудит доступа к данным должен входить в функционал средств информационной безопасности. Помимо этого, программы, которые компания решила использовать, должны включать следующие опции:

- аутентификация и идентификация при входе в систему;
- контроль допуска к информации для пользователей разных уровней;
- обнаружение и регистрация попыток НСД;
- контроль работоспособности используемых систем защиты информации;
- обеспечение безопасности во время профилактических или ремонтных работ.

8 Объекты и предмет защиты в организации

Основными объектами защиты на предприятии являются:

1. персонал (так как эти лица допущены к работе с охраняемой законом информацией (производственные 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;
3. информация ограниченного доступа, а именно:

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

4. защищаемая от утраты общедоступная информация:

- документированная информация, регламентирующая статус предприятия, 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, данные клиентов, электронные базы данных работников, 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 Windows, шифрование);

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

- база данных о клиентах и сотрудниках предприятия 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.

9 Угрозы защищаемой информации в организации

Проблемы, которые включают в себя безопасность АЗС можно разделить на 2 основные части; защита от внешних угроз, защита от внутренних угроз.

Внешние угрозы:

- ДТП;
- вандализм (порча имущества, обрыв пистолетов для заправки, др.);
- разбойные нападения;
- мошенничество;
- катаклизмы;
- технологические происшествия (напр., возгорание);
- кражи в магазине сопутствующих товаров.

Внутренние угрозы:

- манипуляции с чеками (аннулирование, подмена, скидки и т.д.);
- манипуляции с талонами;
- сговор с мошенниками;
- кражи;
- манипуляции с топливом.

10 Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию в организации

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.

11 Каналы и методы несанкционированного доступа к защищаемой информации в организации

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.

12 Основные направления, методы и средства защиты информации в организации

Видеосистема

Видеонаблюдение является доминирующей системой сбора информации и должно фиксировать наиболее важные события для обеспечения безопасности на АЗС, такие как:

- операции, связанные с оборотом наличных денег, к примеру, все позиции и данные чека, операции со скидочными (дисконтными) картами, а также с безналичными формами оплаты (в том числе с нулевыми чеками);
- технологические операции на рабочем месте оператора: отпуск топлива (тех-пролив), сброс транзакции и т.п.;
- контроль проведения инвентаризации товарно-материальных ценностей на АЗС/АЗК;

- прием и хранение нефтепродуктов, наложение на видеоизображение данных резервуарного парка, фиксирование государственного регистрационного знака бензовоза;
- начало и окончание слива нефтепродуктов.

Для осуществления указанных функций системе видеонаблюдения нужно располагать всем необходимым "инструментарием": возможностью мгновенного доступа к списку записей в режиме архива, способностью осуществлять синхронное воспроизведение из архива по нескольким видеокамерам и экспортировать видеоархив в формат AVI (для просмотра на компьютере или бытовом DVD-проигрывателе), а изображения - в формат JPEG. Алгоритм компрессии видеоизображения должен обеспечивать высокое качество изображения с разрешением не менее 704x288, кроме того, необходим алгоритм, устраняющий эффект "гребенки" для кадра максимального разрешения и не вносящий искажение и уменьшение реального размера кадра.

Система видеонаблюдения должна иметь возможность удаленного мониторинга и администрирования в случае применения комплекса на ряде АЗС, немаловажным может быть применение интеллектуальных детекторов, таких как детектор оставленных предметов (неправильной парковки), детектор масок (нападения на АЗС/АЗК обычно осуществляются грабителями в масках).

Специализированные видеомодули, такие как "Авто" (регистрация транспортных номеров) и POS (учет кассовых операций), дадут возможность обеспечивать качественную работу "математики", сбор и хранение данных обо всех событиях, происходящих в зоне контроля, а также возможность подключения к заранее созданным базам данных.

Наличие возможности анализа видеоархива и его качество также очень важны, потому что работа с данными системы видеонаблюдения часто происходит после того, как событие произошло (по принципу ретроспективного анализа). Следовательно, должны поддерживаться следующие функции: мгновенный доступ к любому кадру, выборочный просмотр и анализ действий оператора на конкретной кассе при различных кассовых операциях, анализ всех событий за указанный период времени.

Для наиболее полного контроля обстановки на территории автозаправочного комплекса можно расположить видеокамеры следующим образом:

Внутренние видеокамеры:

- на входе в помещение торгового зала (для обеспечения качественной визуальной идентификации личности);
- в пространстве, прилегающем к стеллажам с предметами торговли;
- на рабочих местах (возможность идентификации как кассира, так и клиента);
- в кафетерии;
- у походов к двери запасного выхода;

Внешние видеокамеры:

- в местах заправки автомашин (для обеспечения идентификации государственных номеров автомашин);
- у площадки слива топлива из автоцистерн;
- на территории въезда/выезда с/на АЗС/АЗК;
- у площадки самообслуживания (например, возле места для самостоятельной накачки шин);
- в местах парковки автотранспорта клиентов и сотрудников;
- над дверью запасного выхода из здания АЗС и местом подвоза товара.

Система электронной защиты от краж товаров в мини-маркете при АЗС/АЗК

Последние исследования и опросы показали, что на автозаправочном комплексе выгодно содержать магазин. Люди, приехавшие заправить свой автомобиль, охотно приобретают еще и продукты, сопутствующие товары. Объяснение этому простое: каждый стремится сэкономить время, поэтому делать дополнительную остановку для покупки еды, автозапчастей и автохимии не имеет смысла, если все это можно купить на АЗС.

Лучший способ для этого - открыть магазин самообслуживания. Но именно они наиболее привлекательны для тех, кто хочет что-либо взять не заплатив. Система защиты товаров от краж должна работать круглосуточно в режиме контроля и осуществлять звуковое оповещение персонала в случае выноса неоплаченных товаров из торгового зала.

Оборудование приема-передачи тревожной сигнализации на централизованный пульт охраны

Для подачи сигнала тревоги на пульт централизованной охраны территориального отдела вневедомственной охраны и/или в дежурную часть органов внутренних дел о хулиганских действиях и возникновении угрозы на АЗС/АЗК они должны быть оборудованы тревожными извещателями (кнопками, радиокнопками, радиобрелоками и прочими устройствами).

Система голосового оповещения

Система голосового оповещения широко применяется на АЗС и предназначена для оперативного информирования персонала и клиентов о возникшей или приближающейся внештатной ситуации (аварии, пожаре, нападении).

Системы охранной и охранно-пожарной сигнализации, контроля доступаСистему охранной сигнализации на АЗС можно разделить на две части. Первая нужна для охраны периметра здания, входных дверей охраняемых помещений, погрузочно-разгрузочных люков, окон, остекленных конструкций охраняемых помещений. Вторая - для защиты помещения изнутри от проникновения, а также для охраны сейфов и шкафов, которые содержат различные товарно-материальные ценности.

Системы контроля и управления доступом (СКУД) и охранно-пожарной сигнализации (ОПС) должны постоянно собирать информацию о зафиксированных сработках пожарных или охранных датчиков, открытиях или

закрытиях замков, управляемых СКУД. При потере связи с управляющим сервером системы должны накапливать информацию о событиях и передать ее на него после восстановления связи.

Время прихода сотрудника на работу, время ухода, а также контроль входа в различные помещения АЗС контролируются СКУД и могут сохраняться в ее памяти. При помощи специализированных приложений время присутствия сотрудника на рабочем месте сравнивается с его индивидуальным графиком работы, выявляя опоздания и преждевременные уходы с работы. СКУД и ОПС должны иметь интеграцию с видеосистемой, что позволит быстрее находить определенные события в архиве и иметь визуальную информацию, полученную с видеокамер, установленных в зоне точек прохода СКУД. Чтобы войти в подсобное помещение (или выйти из него), сотрудник АЗС должен будет поднести свою карту доступа к считывателю или набрать личный код. Только после этого он сможет открыть дверь.

Комплекс и входящий в его состав сервер формирования БД СКУД и ОПС предназначены для:

- управления контролем доступа;
- фиксации информации, связанной с управлением доступом (открытие/закрытие дверей);
- контроля состояния датчиков ОПС;
- передачи сигналов тревоги на различные устройства оповещения (звуковые и световые).
- ведения протокола событий.

Система пожарной сигнализации

Что дает интеграция ОПС с другими подсистемами безопасности распределенной системы? Это позволяет программировать необходимые виды реакции пожарной сигнализации на события, поступающие от устройств, входящих в ее состав, дает возможность автоматического, заранее запрограммированного по некоему тревожному алгоритму управления исполнительными устройствами - средствами оповещения, блокировки и отпирания дверей и т.д. Немаловажным фактором является возможность объединения исполнительных устройств различных подсистем

ОПС в группы, что позволяет, к примеру, выводить единый план охраняемых помещений с удобным для оператора представлением расположения устройств ОПС и их статуса на единый монитор.

13 Выводы

В процессе выполнения практического задания была поставлена задача разработать СОИБ для АЗС «Альфа».

Эта цель была достигнута. Были определены цели и задачи разработки системы безопасности на предприятии, определены права доступа для сотрудников, выявлены предметы и объекты защиты, угрозы (внешние и внутренние), а также были предложены методы по и средства защиты информации в организации.