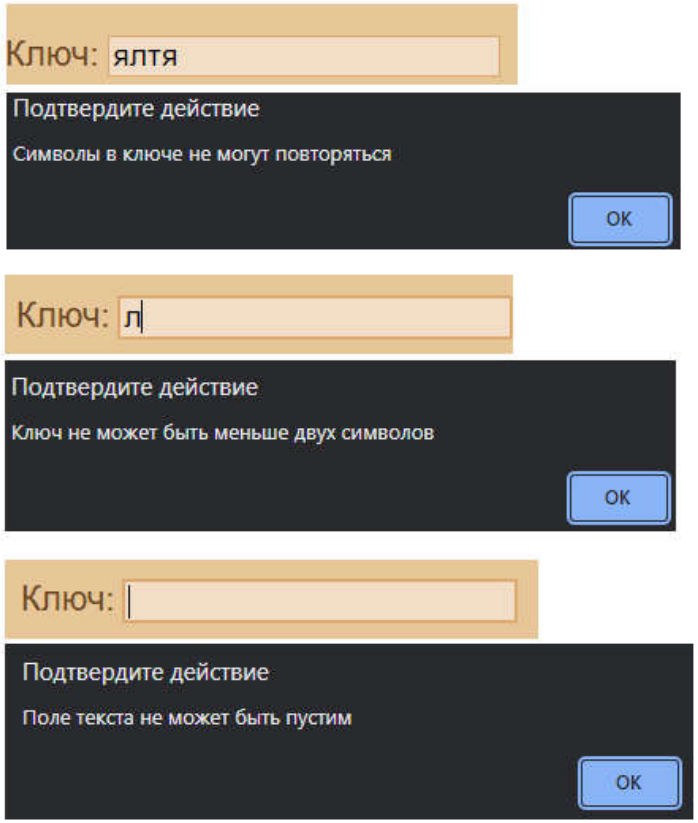
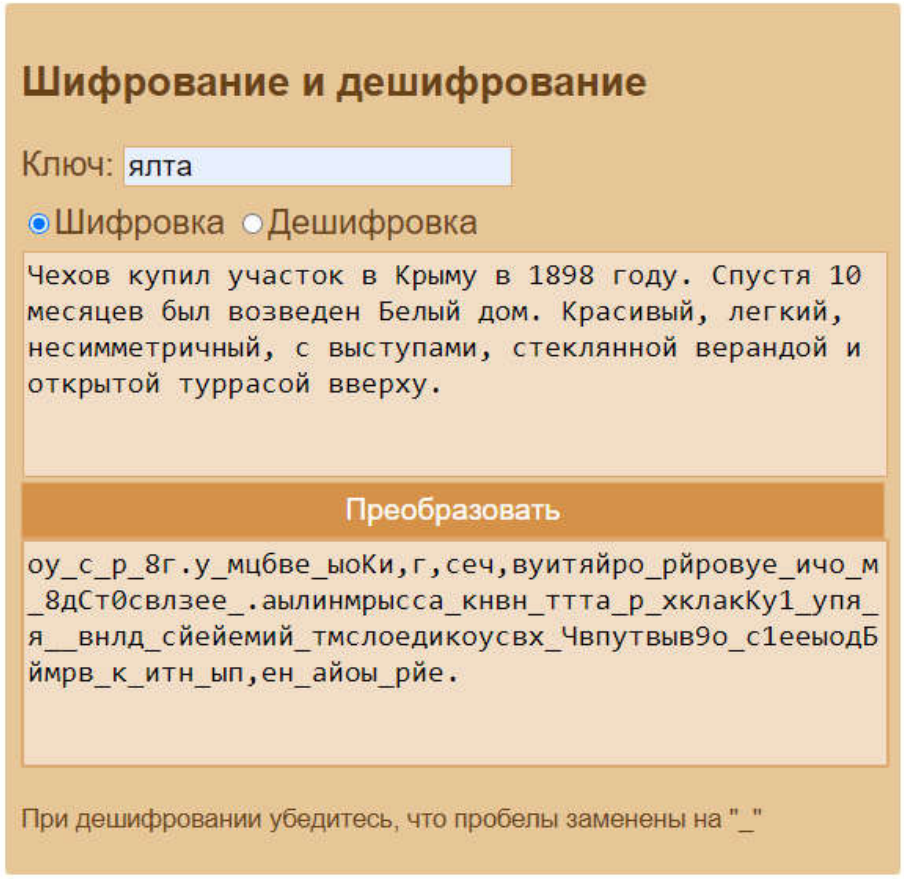
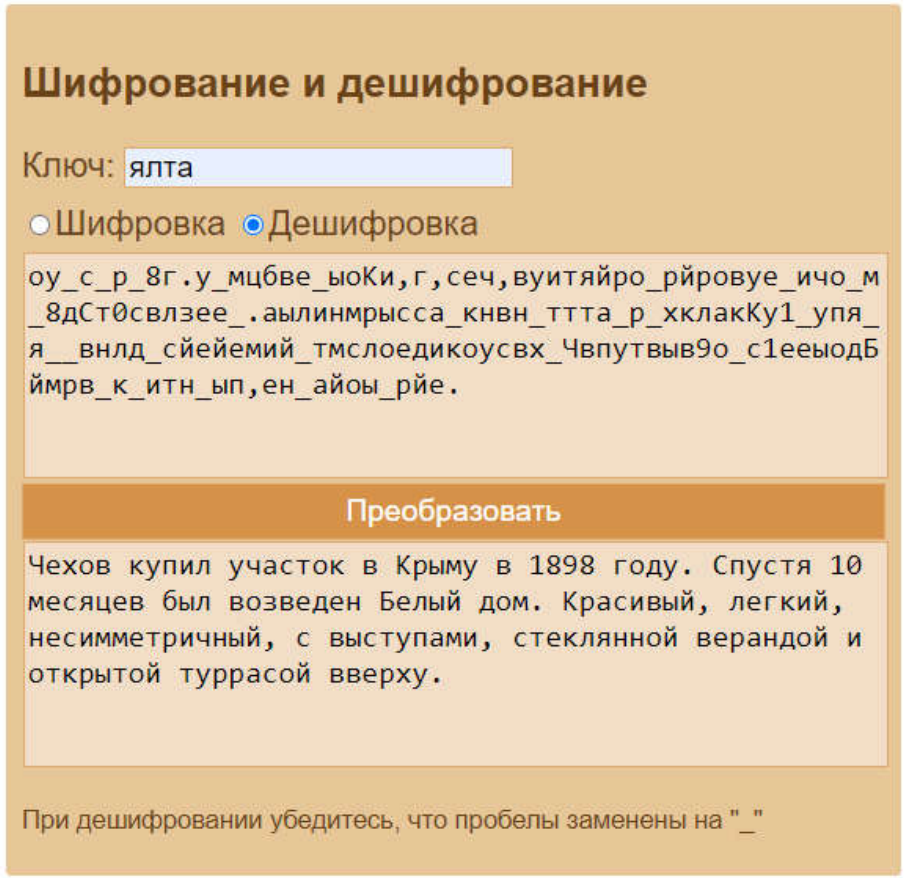
Практическое занятие № 3

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 перестановки один из самых старых и часто встречаемых методов шифрования. Шифр перестановки заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Шифрование простой перестановкой (вертикальной перестановкой) осуществляется следующим образом: 1) выбирается ключевое слово с неповторяющимися символами; 2) шифруемый текст записывается последовательными строками под символами ключевого слова; 3) зашифрованный текст выписывается колонками в той последовательности, в которой располагаются в алфавите буквы ключа (или в порядке следования цифр в натуральном ряду, если ключ цифровой).
2	Используя любой язык программирования разработать программный продукт.	В ходе выполнения практической работы необходимо создать приложение для шифрования и дешифрования текста. Для этого были выбраны JavaScript и HTM.
3	Произвести его оптимизацию.	

4	Произвести отладку программы.	
5	Произвести тестирование программы.	





7. Контрольные вопросы:
   1. Какие языковые конструкции использованы в программе: indexOf, sort, split, ceil, length, floor
   2. Использовались ли процедуры и функции? Описать их назначение.
      Созданы три функции: encode и decode для шифрования и дешифрования текста, doIt срабатывает при нажатии на кнопку, проверяет ключ и запускает процесс шифрования\дешифрования.
   3. Используя листинг программы, пояснить работу операторов выполняющих ключевые функции программы.

```
function encode(){
  var inputKey = document.getElementById('input-key');
  var input1 = document.getElementById('input1');
  var output1 = document.getElementById('output1');
  var key = inputKey.value;
  var text = input1.value;
```

```
  var mat = [[]];
  var chars = []; // Массив для раскладки позиций букв
  var ar = key.split('').sort();//Буквы ключа в алфавитном порядке
  var shirina = key.length;
  var visota = Math.ceil(text.length / key.length);
  var y = 0, x = 0;
  var output = '';
  for (var i = 0; i < text.length; i++) { //Заполнение матрицы
    mat[y][x] = text[i]; x++;
    if(x > shirina-1 && i < text.length-1){
      x = 0; y++;
      mat[y] = [];
    }
  }
  for (var i = 0; i < ar.length; i++) {//Размещение очередности в массиве
    var pos = key.indexOf(ar[i]);
    chars[pos] = i;
  }
  for (var i = 0; i < shirina; i++) {//Формирование кодированного сообщения
    for (var j = 0; j < visota; j++) {
      var pos = chars.indexOf(i);
      if(mat[j][pos] != undefined){
        if (mat[j][pos] != ' ')
        output+= mat[j][pos];
        else output+= '_';
      }else{
        output+= mat[j][pos] =  '';
      }
    }
  }
  output1.value = output;
}

function decode(){
  var inputKey = document.getElementById('input-key');
  var input1 = document.getElementById('input1');
  var output1 = document.getElementById('output1');
  var key = inputKey.value;
  var text = input1.value;
```

```
var mat = [[]];
var shirina = key.length;
var visota = Math.ceil(text.length / key.length);
var bottomRow =  shirina - (shirina * visota - text.length);
var ar = key.split('').sort(); //алфавитный порядок символов ключа
var chars = [];
var output = '';
for (var i = 0; i < visota; i++){//Создание матрицы
  if(i < Math.floor(text.length / shirina)){
    mat[i] = new Array(shirina)
  }else{
    mat[i] = new Array(bottomRow);
  }
}
for (var i = 0; i < ar.length; i++) {
  var pos = key.indexOf(ar[i]);
  chars[pos] = i;
}
var position = 0;
for (var i = 0; i < shirina ; i++) { //Заполнение матрицы
  for (var j = 0; j < visota; j++) {
    var pos = chars.indexOf(i)
    if( j*shirina + pos < text.length  ){
      mat[j][pos] = text[position];
      position++;
    }
  }
}
for (var i = 0; i < visota; i++) { //Формирование строки дешифрованного текста
  for (var j = 0; j < shirina; j++) {
    var bukva = mat[i]?.[j];
    if(bukva != undefined){
      if(bukva == '_')
        output += ' ';
      else output+= bukva;
    }
  }
}
output1.value = output;
```

```
}
```

7. Выводы о проделанной работе: в ходе практического занятия создано приложения на языке JS для шифрования\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, MS Office, 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. Ознакомится 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?
   - Является ли процедура построения СОИБ циклической? Обоснуйте Ваш ответ.
   - Дайте характеристику современным злоумышленникам, совершающим правонарушения в сфере информационной безопасности.
   - Обоснуйте необходимость проведения регулярной работы с сотрудниками организации.
   - Какова конечная цель полученной СОИБ?

8. Выводы о проделанной работе.

1. Описание предприятия

ООО «Полесье».

Основной вид деятельности - 25.30.2 «Производство ядерных установок и их составных частей, в том числе для транспортных средств».

Основной деятельностью предприятия является конструирование и изготовление оборудования для атомной энергетики, традиционной энергетики, нефтегазового комплекса, металлургии и других отраслей промышленности.

Пользователей – 300.

Компьютеров – 310.

Режим многопользовательский.

Есть выход в интернет.

Система распределенная.

Обрабатываемых данных больше 10 000 и меньше 50 000.

Нужно защитить персональные данные.

Предприятие включает в себя следующие отделы:

1. Отдел логистики;
2. Отдел кадров;
3. Планово-экономический отдел;
4. Бюро инструментального хозяйства;
5. Планово-распределительное бюро;
6. Отдел кооперации;
7. Отдел материально-технического снабжения;
8. Отдел технического контроля;
9. Отдел информационных технологий;
10. Отдел качества;
11. Отдел маркетинга;
12. Бухгалтерия.

Уровни конфиденциальности:

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

На предприятии имеются следующие должности:

1. директор;
2. главный бухгалтер;
3. энергетик;
4. системный администратор;
5. кадровик;
6. сварщик;
7. менеджер по работе с персоналом;
8. менеджер отдела кадров;
9. грузчик;
10. кладовщик.

Характеристика информационной системы предприятия

ООО «Полесье» использует следующее программное обеспечение:

-пакет MicrosoftOffice;

-1С Предприятие 8;

-Компас 3D (программа автоматизированного проектирования);

-AutoCad (программа автоматизированного проектирования и черчения);

-RAdmin (программа для удаленного доступа к компьютеру);

Персональный компьютер есть у каждого работника предприятия.

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.

Актуальность проблемы защиты информации на предприятии

Обеспечение защиты информации на предприятии предусматривает необходимость защиты производственных данных. Наиболее важной представляется защита производственных данных, так как доверие заказчиков в первую очередь основывается на предоставлении своих данных, и соответственно, сохранением их сотрудниками предприятия.

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

Задачи

В данном индивидуальном задании практиканта поставлены следующие задачи:

9. Определить цели и задачи защиты информации на предприятии;
10. Составить матрицу доступа;
11. Определить группу требований к автоматизированной системе (далее будет использовано сокращение ас);
12. Определить предмет защиты на предприятии;
13. Выявить возможные угрозы защищаемой информации на предприятии и их структуру;
14. Выявить источники, виды и способы дестабилизирующего воздействия на защищаемую информацию на предприятии;
15. Выявить каналы и методы несанкционированного доступа к защищаемой информации на предприятии;
16. Определить основные направления, методы и средства защиты информации на предприятии.

2. Цели и задачи защиты информации на предприятии

Целями защиты информации предприятия являются:

– предупреждение хищения, утечки, утраты, искажения, подделки конфиденциальной информации (персональных данных);

– предотвращение угроз безопасности личности и предприятия;

– 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, имеющихся в информационных системах;

– сохранение, конфиденциальности документированной информации в соответствии с законодательством.

К задачам защиты информации на предприятии относятся:

– обеспечение управленческой, финансовой и маркетинговой деятельности предприятия 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 предприятию преимущества перед конкурентами 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 предприятия;

– 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 на предприятии являются:

O1 – технические средства приема, передачи и обработки информации;

O2 – производственные данные заказчиков;

O3 – персональные данные работников;

O4– документированная информация;

O5 – личные дела работников;

O6 – электронные базы данных работников и заказчиков;

O7 – средства защиты информации (антивирусные программы, система сигнализации, система противопожарной охраны и др.);

Субъектами доступа к ресурсам предприятия являются:

S1 – директор;

S2 – главный бухгалтер;

S3 – энергетик;

S4 – системный администратор;

S5 – кадровик;

S6 – менеджер по работе с заказчиками;

S7 – менеджер отдела кадров;

S8 – грузчик;

S9 – кладовщик;

S10 – сварщик;

Таблица 1. Матрица доступа

	O1	O2	O3	O4	O5	O6	O7
S1	R	R	R,W	R,W	R	R	R
S2	-	R,W,CR,D	R	R,W, CR, D	R	R,W,CR,D	-
S3	-	-	-	R,W, CR, D	-	-	-
S4	R,W, CR, D	R,W, CR, D	R,W, CR, D	R,W, CR, D	R,W, CR, D	R,W, CR, D	R,W, CR, D
S5	-	-	R,W, CR, D	R,W, CR, D	R,W, CR, D	R,W, CR, D	-
S6	-	R,W, CR, D	R	R,W, CR, D	R	R, CR	-
S7	-	-	R,W, CR	R,W	R,W, CR	R	-
S8	-	R	-	R	-	R	-
S9	-	R	-	R,W, CR, D	-	R	-
S10	-	R	-	R,W, CR, D	-	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 предприятия, 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 на предприятии

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, 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);
- производственные данные заказчиков(ИНН, название организации, ФИО представителя, адрес доставки, юридический адрес, контактный телефон, история заказов);

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, личные дела заказчиков, электронные базы данных работников и заказчиков, 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);
7. технологические отходы (мусор), образовавшиеся в результате обработки охраняемой законом информации (данные о бывших заказчиках и сотрудниках).

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

- база данных о заказчиках 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.

6. Угрозы защищаемой информации на предприятии

Внешние угрозы:

- конкуренты;
- 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 предприятия;
- нарушение целостности данных со стороны персонала предприятия;
- потеря информации на жестких носителях;
- угрозы целостности баз данных;
- угрозы целостности программных механизмов работы предприятия;
- 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 на предприятии

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.

8. Организация комплексной системы защиты информации на предприятии

Для обеспечения защиты информации, содержащейся в информационной системе, на предприятии 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»

Защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы (далее - система защиты информации информационной системы).

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 предприятия можно было защитить свои права юридически и наказать нарушителя.

Программа будет отражать размер данного предприятия, тип технологии и деловой информации, которую необходимо защищать.

В программе должны учитываться возможные источники и каналы утечки информации.

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

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 секретных работ. 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 ведутся секретные работы.

Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

1. Идентификацию и аутентификацию субъектов доступа и объектов доступа;
2. Управление доступом субъектов доступа к объектам доступа;
3. Ограничение программной среды;
4. Защиту машинных носителей информации;

5. Регистрацию событий безопасности;
6. Антивирусную защиту;
7. Обнаружение (предотвращение) вторжений;
8. Контроль (анализ) защищенности информации;
9. Целостность информационной системы и информации;
10. Доступность информации;
11. Защиту среды виртуализации;
12. Защиту технических средств;

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 прегражденияя доступа посторонних лиц к носителям защищаемой информации.

Заключение

В процессе выполнения индивидуального задания практикантами была поставлена задача – создать и проанализировать средства информационной безопасности предприятии ООО «Полесье». Поставленные цели были достигнуты при помощи классифицирования предприятия, были предложены методы и средства для усовершенствования политики безопасности данного предприятия, в результате выполнения которых предприятие 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 предприятие циркулирует большим 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.