

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Локтионова Оксана Геннадьевна  
Должность: проректор по учебной работе  
Дата подписания: 06.06.2024 14:49:29  
Уникальный программный ключ:  
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

## МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное  
учреждения высшего образования

«Юго-Западный государственный университет»  
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ

Проректор по учебной работе

О.Г. Локтионова

« 16 » 05

2024 г.



### Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем

Методические указания по выполнению практических работ по  
дисциплине «Экспертные системы комплексной оценки  
безопасности информационных и телекоммуникационных систем»  
для студентов направления подготовки 10.04.01 «Информационная  
безопасность»

Курск 2024

УДК 004

Составители: Таныгин М.О

Рецензент

Кандидат технических наук, доцент кафедры  
вычислительной техники А.В. Киселев

**Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем:** методические указания по выполнению практических работ / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2024. – 23 с.: Библиогр.: с. 23.

Содержат сведения по вопросам анализа информации на предприятии. Указывается порядок выполнения практических работ, правила оформления, содержание отчета.

Методические указания по выполнению практических работ по дисциплине «Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем» предназначены для студентов направления подготовки 10.04.01 «Информационная безопасность».

Текст печатается в авторской редакции  
Подписано в печать 16.05.24 . Формат 60x84 1/16.  
Усл. печ. л. 12. Уч. – изд. л. 1,1. Тираж 50 экз. Заказ 413  
Бесплатно.

Юго-Западный государственный университет.  
305040, г. Курск, ул. 50 лет Октября, 94.

# Практическая работа №1 на тему: «Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации».

## Задание

Ознакомиться с принципами системного подхода при создании структуры ГОСТ и ИСО.

### 1. Порядок выполнения работы:

1. Произвести поиск всех существующих государственных и международных стандартов в области информационных технологий, информационной безопасности и защиты информации. При нахождении – вносить в универсальный каталогизатор дисков, файлов, папок, а также любых нефайловых элементов wincatalog<sup>1</sup>.

Пример заполнения приведен на рисунке 1.

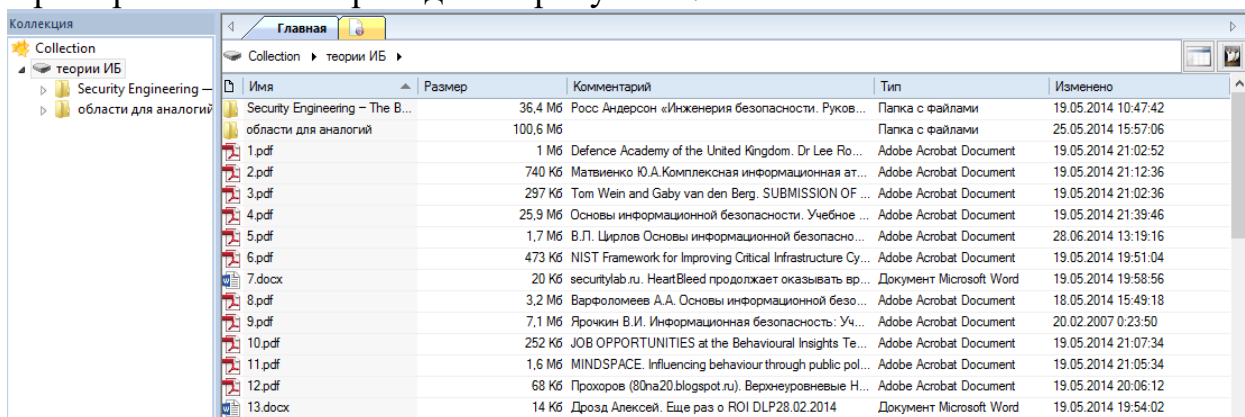


Рис.1 – Пример внесения документов в универсальный каталогизатор

2. При заполнении присваивать теги, которые описывают данный документ или область его применения, для последующей группировки.

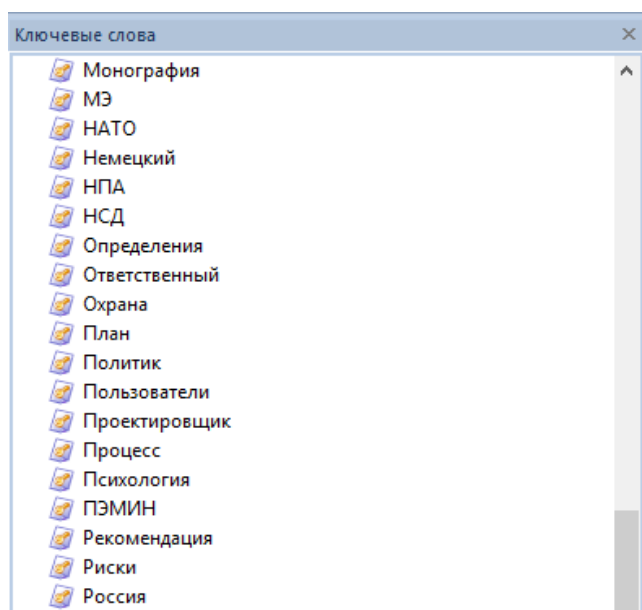
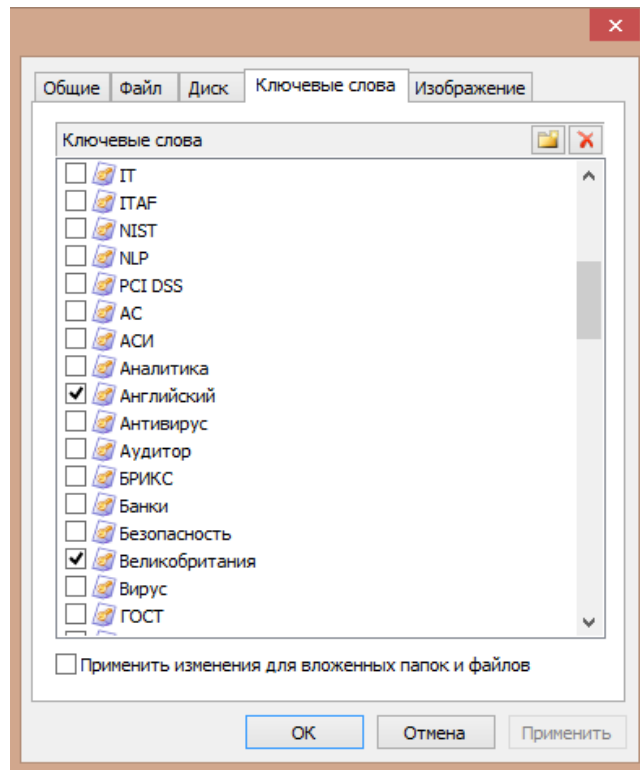


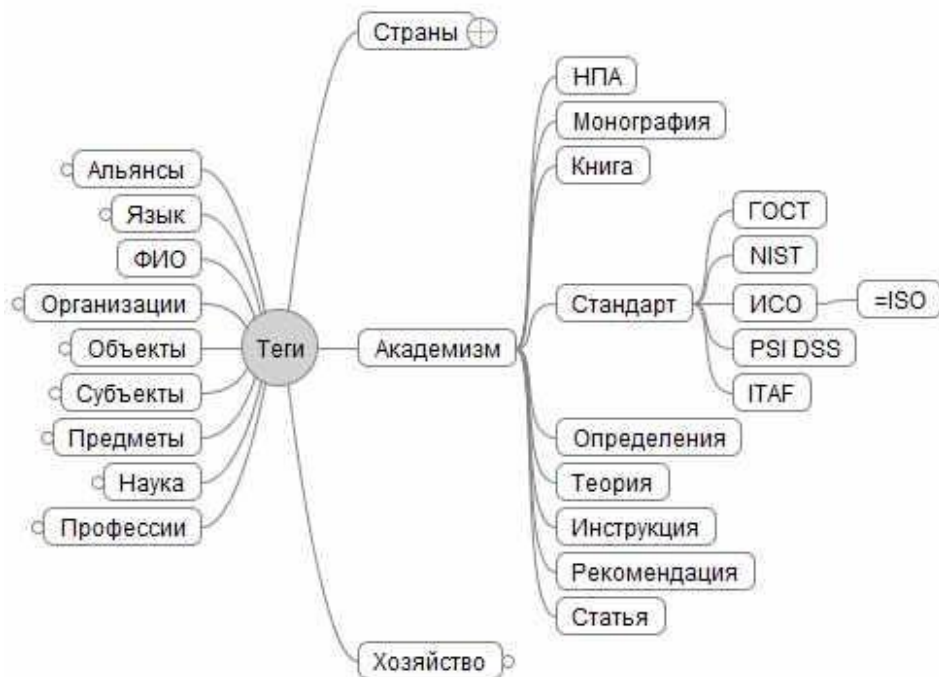
Рис.2 – Пример создания списка тегов

<sup>1</sup> <http://www.wincatalog.com/ru/>



**Рис.3 – Пример присваивания тегов документу**

3. После заполнения системы тегов – необходимо графически их представить с помощью программы FreeMind<sup>2</sup> или аналога.



**Рис.4 – Пример графического представления тегов**

4. На основе полученных данных - заполнить таблицу с перечнем найденных ГОСТ и ИСО по приведенному примеру:

<sup>2</sup> <http://sourceforge.net/projects/freemind/>

**Таблица 1 – Список стандартов**

<b>№ п/п</b>	<b>Номер стандарта</b>	<b>Статус</b>
<b>Защита сетей общего пользования</b>		
<b>1.</b>	ГОСТ Р 53110-2008	Действует
<b>2.</b>	ГОСТ Р 53111-2008	Действует
<b>3.</b>	ГОСТ Р 53109-2008	Действует
<b>Оценка безопасности автоматизированных систем</b>		
<b>4.</b>	ГОСТ Р ИСО/МЭК ТО 19791-2008	Действует
<b>5.</b>		

5. Составить отчет. В отчете должны быть представлены четко видные и понятные скрины экрана при выполнении работы и оформленная таблица.
6. Найти нужно как можно больше стандартов.

**Список дополнительной литературы:**

1. Справочно-поисковая система «Консультант Плюс»;
2. Справочно-поисковая система «Гарант»;
3. Федеральное агентство по техническому регулированию и метрологии;
4. Международная организация по стандартизации.

**Практическая работа №2**  
**на тему: «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности».**

## Цель работы

Целью данной лабораторной работы является обзорного документа по сертифицированным продуктам в заданной области информационной безопасности.

## Требования к выполнению задания:

В ходе выполнения задания необходимо провести анализ сертифицированных продуктов в заданной области информационной безопасности. После этого следует определить, какие средства защиты являются наиболее приемлемыми для использования в системах защиты. По результатам анализа оформить отчет.

При поиске средств защиты в заданной области, искать сертификацию на соответствие требованиям:

№	Вид СЗИ	Предназначение средства (область применения)
1.	Средства защиты от несанкционированного доступа	соответствует документу «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа»
2.	Межсетевые экраны	соответствует документу «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатель защищенности от несанкционированного доступа к информации»
3.	Антивирусные средства	соответствует документу «Требования к средствам антивирусной защиты»
		соответствует документу «Профиль защиты средств антивирусной защиты»
4.	Средства криптографической защиты	«может использоваться для криптографической защиты»
5.	Средства обнаружения вторжений	соответствует документу «Требования к системам обнаружения вторжений»
		соответствует документу «Профиль защиты систем обнаружения вторжений уровня узла»
6.	Средства контроля защищенности (автоматизированного анализа защищенности и обнаружения уязвимостей автоматизированных систем)	«является средством анализа защищенности и обнаружения уязвимостей»

№	Вид СЗИ	Предназначение средства (область применения)
7.	Средства резервного копирования	«предназначен для создания автоматизации процессов резервного копирования»

### 1. Задание:

Примерный перечень заданий:

1. Определить, кто из регуляторов проводит сертификацию в заданной области средств защиты информации
2. Пользуясь сайтами регуляторов в области защиты информации Федеральной службы безопасности (<http://clsz.fsb.ru/>) и Федеральной службы по техническому и экспортному контролю (<http://fstec.ru/>) выбрать средства защиты по направлению (номер в списке группы по порядку):
  - 2.1. Средства защиты от несанкционированного доступа;
  - 2.2. Межсетевые экраны;
  - 2.3. Антивирусные средства;
  - 2.4. Средства криптографической защиты;
  - 2.5. Средства обнаружения вторжений;
  - 2.6. Средства контроля защищенности;
  - 2.7. Средства резервного копирования;
  - 2.8. Свой вариант (по согласованию).
3. Сделать сравнительный анализ всех средств защиты в форме таблицы.

№	Название	Срок действия	Выполняемые функции	Изготовитель
---	----------	---------------	---------------------	--------------

4. Из полученного списка и определить наиболее привлекательные средства защиты. Объяснить почему.
5. Найти сертификаты для выбранных средств защиты информации (на сайтах производителей).
6. Сопоставить данные из сертификата выбранного средства защиты и требования руководящего документа Гостехкомиссии или другого соответствующего документа (найти ссылку в сертификате).

### 2. Требования к отчету:

Отчет должен содержать:

1. титульный лист;
2. цель работы;
3. заданную область информационной безопасности;
4. сравнительный анализ средств защиты;
5. выбранное оптимальное средство защиты, обоснование почему и сертификат на него (скачать на сайте производителя СЗИ);
6. Перечень документов, на соответствие которым сертифицирован продукт;
7. выводы по проделанной работе.



### **3. Вопросы:**

1. Как проводится сертификация средств защиты информации?
2. Что показывают характеристики данного средства защиты?
3. Какой регулятор контролирует данную область информационной безопасности?
4. Какая основная информация содержится в сертификате?

### **Список дополнительной литературы:**

1. Справочно-поисковая система «Консультант Плюс»;
2. Справочно-поисковая система «Гарант»;
3. <http://clsz.fsb.ru/>
4. <http://fstec.ru/>

**Практическая работа №3 на тему: «Анализ заданного  
нормативно-правового акта Российской Федерации».**

## **Цель работы**

Целью данной лабораторной работы является знакомство с нормативно-правовыми актами и законодательством Российской Федерации, регулирующим вопросы защиты информации.

## **Требования к выполнению задания:**

В ходе выполнения задания необходимо провести анализ заданного нормативного документа. Действия выполнять в следующем порядке:

1. определить какая цель в разборе документа;
2. определить статус документа по отношению к вашей задаче;
3. определить сферу действия документа;
4. определить входит ли в сферу действия документа;
5. определиться с размером шрифта для комфортного чтения и отформатировать так, чтобы по возможности не «разрывать» статьи на несколько страниц и при склейке статья не оказалась на разных строках склейки;
6. распечатать на 1 стороне;
7. склеить по ширине так, чтобы верхняя часть оказалась не выше 15 см от макушки, а нижняя не ниже живота;
8. прочитать;
9. пронумеровать все списки (если они не были пронумерованы);
10. преобразовать все классификации и требования для разных случаев в таблицы;
11. при втором прочтении разбить на блоки по смыслу или задаче;
12. каждому блоку придумать название, состоящее из одного слова и несущее смысл его содержания (можно использовать символы);
13. каждому блоку назначить свой цвет (стоящие рядом цвета должны быть не смешиваемыми);
14. запомнить количество блоков;
15. запомнить названия блоков и их цвета;
16. составить иерархическую систему или интеллект карту<sup>1</sup>;
17. повторить пункты 10, 12, 13 и 14 для каждого абзаца в блоке;
18. при следующем прочтении найти и выписать все отсылки вверх (с указанием пункта откуда взято требование);
19. при следующем прочтении найти и выписать все отсылки вниз (с указанием пункта откуда взято требование);
20. при следующем прочтении найти и выписать все отсылки в стороны (с указанием пункта откуда взято требование);
21. составить иерархическую систему или интеллект карту нормативных актов
22. переформатировать блоки под свою задачу;
23. перепечатать и склеить заново по смыслу или задаче;
24. повторить пункт 11.

---

<sup>1</sup> FreeMind скачать по адресу <http://sourceforge.net/projects/freemind/>

**За одно прочтение можно выполнять ТОЛЬКО одно действие!**

**Задание:**

Примерный перечень заданий (в соответствии с номером в списке в группе):

1. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;
2. Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи»;
3. Федеральный закон от 04.05.2011 №99-ФЗ «О лицензировании отдельных видов деятельности»;
4. Приказ ФСТЭК России от 11.02.2013 №17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах";
5. Приказ ФСТЭК России от 18.02.2013 №21 "Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";
6. Приказ ФСТЭК России от 14.03.2014 №31 "Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды";
7. Приказ ФСБ России от 10.07.2014 №378 "Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности"
8. Постановление Правительства РФ от 15.08.2006 №504 «О лицензировании деятельности по технической защите конфиденциальной информации»;
9. Приказ ФСБ РФ №416, ФСТЭК РФ №489 от 31.08.2010 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования».

**Требования к отчету:**

Отчет должен содержать:

1. титульный лист;
2. цель работы;
3. полученные блоки, на который разбит НПА;
4. интеллект-карту нормативного документа;
5. приложенный распечатанный, склеенный документ с выделенными блоками;
6. вывод по работе.

**Вопросы:**

1. Какие части документа относятся к вопросам защиты информации?
2. Что показывают комментарии к данному документу?
3. Как менялся текст нормативного акта с момента его создания по настоящее время?

**Список дополнительной литературы:**

1. Справочно-поисковая система «Консультант Плюс»;
2. Справочно-поисковая система «Гарант».

**Практическая работа №4 на тему: «Определение класса  
государственной информационной системы (ГИС)».**

## Оглавление

Цель работы .....	3
1. Требования к выполнению задания: .....	3
2. Задание: .....	3
3. Теория.....	4
4. Ход работы .....	8
5. Вопросы.....	9
Список дополнительной литературы .....	9

## **Цель работы:**

научиться определять класс государственной информационной системы (ГИС).

### **1. Требования к выполнению задания:**

Ознакомиться и изучить основные принципы разработки организационно-правовых аспектов деятельности службы защиты информации.

### **2. Задание:**

1. В соответствии с предложенным вариантом организации или предприятия проанализировать организационно-правовое обеспечение защиты информации в системе деятельности предприятия в целом.
2. Выявить существующие проблемные моменты и узкие места.
3. В соответствии с Законом "Об информации, информатизации и защите информации", Законом Российской Федерации "О безопасности" описать основные подходы к разработке организационно-правового обеспечения службы защиты информации на выбранном предприятии.
4. Определить круг задач службы защиты информации (СЗИ).
5. Сформулировать основные функции СЗИ.
6. Выделить в организационно-штатной структуре штатные единицы, обеспечивающие реализацию данных функции и особенности взаимодействия между собой.
7. Проанализировать нормативное обеспечение деятельности СЗИ, выявить проблемы.
8. Сформировать общую структуру нормативной документации по обеспечению безопасности информации в организации в следующей иерархии:
  - Документы концептуального уровня, которые должны быть разработаны руководителями организаций;
  - Документы общего уровня (применения);
  - Документы, регламентирующие работу персонала с защищаемыми носителями.
9. Разработать отсутствующие документы, опираясь на законодательную базу, указанную в списке литературы, а также, используя Гарант, Консультант-Плюс. Доработать несоответствующие требованиям законодательства документы.

Разработать:

- 1) Положение о подразделении по защите информации. Общее руководство по руководству, функциям, задачам, правам, обязанностям, ответственности и штатной структуре.
- 2) Положение о категорировании ресурсов.

Вопросы для самоконтроля

1. Какие функции выполняет СЗИ предприятия для решения задач защиты информации?



2. Как строится структура полномасштабной системы обеспечения безопасности и защиты информации предприятия?
3. Какова специфика организации и выполнения охранных функций?
4. Каковы суть и содержание нормативной основы организации ЗСИ?
5. Какие факторы влияют на формирование организационно-правового обеспечения защиты информации?
6. Какова структура организационно-правовой основы защиты информации?
7. Опишите организационно-правовые мероприятия по защите конфиденциальной информации.

### **3. Теория**

Защита информационных ресурсов реализуется в рамках нескольких направлений деятельности СЗИ. Это решение научно-технических проблем, правовое регулирование отношений в процессе информатизации деятельности любой организации.

Разработка организационно-правового обеспечения защиты информации является актуальной в связи с признанием за информацией статуса товара, продукта общественного производства, установления в законодательном порядке права собственности на информацию.

Такая постановка вопроса приобретает особый смысл и характер в условиях демократизации общества, формирования рыночной экономики, включения нашего государства в мировое экономическое сообщество. Если решение вопросов развития производственной базы создания средств информатики в какой-то мере можно осуществить с использованием рыночных структур и отношений, то разработка и внедрение законодательной базы информатизации невозможны без активной государственной информационной политики, направленной на построение по единому замыслу организационно-правового механизма управления информационными процессами» увязанного с научно-технической базой информатизации.

Организационно-правовое обеспечение является многоаспектным понятием, включающим законы, решения, нормативы и правила, организационно-распорядительные мероприятия.

Применительно к защите информации, обрабатываемой в информационной системе, данный вид обеспечения имеет ряд принципиальных специфических особенностей, обусловленных следующими факторами, которые показаны на рисунке 1.1.



Рис. 1.1. Факторы, влияющие на формирование организационно-правового обеспечения защиты информации

Исходя из приведенных обстоятельств, комплекс вопросов, решаемых организационно-правовым обеспечением, может быть сгруппирован в три класса:

- организационно-правовая основа защиты информации в информационных системах;
- технико-математические аспекты организационно-правового обеспечения;
- юридические аспекты организационно-правового обеспечения защиты.

Организационно-правовая основа защиты информации должна включать (таблица 1.1).

Таблица 1.1

**Структура организационно-правовой основы защиты информации**

№ п/п	Формирующие составляющие организационно-правовой основы защиты информации в службе защиты информации
1	Определение подразделений и лиц, ответственных за организацию защиты информации
2	Нормативно-правовые, руководящие и методические материалы (документы) по защите информации
3	Меры ответственности за нарушение правил защиты
4	Порядок разрешения спорных и конфликтных ситуаций по вопросам защиты информации

Под технико-математическими аспектами организационно-правового обеспечения понимается совокупность технических средств, математических методов, моделей, алгоритмов и программ, с помощью которых в ИС могут быть соблюдены все условия, необходимые для юридического разграничения

прав и ответственности относительно регламентов обращения с защищаемой информацией. Основными из этих условий являются следующие:

- фиксация на документе персональных идентификаторов ("подписей") лиц, изготовивших документ и (или) несущих ответственность за него;
- фиксация (при любой необходимости) на документе персональных идентификаторов (подписей) лиц, ознакомившихся с содержанием соответствующей информации;
- невозможность незаметного (без оставления следов) изменения содержания информации даже липами, имеющими санкции на доступ к ней,
- т.е. фиксация фактов любого (как санкционированного, так и несанкционированного) изменения информации;
- фиксация факта любого (как несанкционированного, так и санкционированного) копирования защищаемой информации.

Под юридическими аспектами организационно-правового обеспечения защиты информации в ИС понимается совокупность законов и других нормативно-правовых актов, с помощью которых достигаются следующие цели;

- устанавливается обязательность соблюдения всеми лицами, имеющими отношение к информационной системе всех правил защиты информации;
- узакониваются меры ответственности за нарушение правил защиты;
- узакониваются технико-математические решения вопросов организационно-правового обеспечения защиты информации;
- узакониваются процессуальные процедуры разрешения ситуаций, складывающихся в процесс: функционирования систем защиты.

Таким образом, вся совокупность вопросов, возникающих при решении проблем организационно-правового обеспечения, может быть представлена в виде схемы, приведенной на рис.1.2.



Рис. 1.2. Структура Организационно-правового обеспечения защиты информации, формируемого в службе защиты информации

Основополагающим понятием в области правового аспекта защиты информации является “информация”. Закон РФ “Об информации, информатизации и защите информации” определяет понятие информация как “сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления”.

При решении организационно-правовых вопросов обеспечения информационной безопасности исходят из того, что информация подпадает под нормы вещного права, что дает возможность применять к информации нормы Уголовного и Гражданского права в полном объеме.

**Анализ организационно-правового обеспечения** планируемых к осуществлению мероприятий в области организации защиты информации всегда должен предшествовать принятию окончательного решения о реализации этих мероприятий.

К организационно-правовым мероприятиям по защите конфиденциальной информации относятся мероприятия по разработке и принятию определенных документов предприятий и организаций, регламентирующих степень и порядок допуска собственных сотрудников, а также сторонних лиц и организаций к конкретным информационным ресурсам.

Организационно-правовая защита информации реализуется путем установления на предприятии режима конфиденциальности.

Можно выделить три формы конфиденциальных отношений, что представлено в таблице 1.2.

**Таблица 1.2**

**Формы конфиденциальных отношений**

Субъекты отношений	Реализация отношений
Между сотрудником предприятия и самим предприятием как юридическим лицом	Реализуется на практике путем составления соответствующего трудового договора или контракта, заключаемого с сотрудником предприятия
Складывающиеся между конкретным сотрудником и другими сотрудниками этого предприятия	Эти отношения развиваются как по вертикали, так и по горизонтали. Указанные отношения называются конфиденциальными отношениями по служебным функциям. Юридически эти отношения закрепляются многообразными административно-правовыми решениями, например приказами о выполнении определенных работ, и регламентируются “Должностными инструкциями”
Складывающиеся в рамках хоздоговорных работ и базирующиеся на договоре между партнерами	Юридически конфиденциальные отношения закрепляется в виде четко сформулированных требований и обязательств, которые выдвигают договаривающиеся стороны, и фиксируют в договоре

В вопросах реализации технических мероприятий обеспечения информационной безопасности с точки зрения правового обеспечения основное внимание следует уделять выполнению требований лицензирования исполнителей работ и использования сертифицированных средств защиты, а также действующим ограничениям на применение специальных технических средств.

В существующей практике можно выделить следующие основные аспекты решения проблемы защиты информации:

- анализ правового обеспечения;
- реализация организационно-правовых мероприятий защиты;
- реализация технических мероприятий по защите информации.

Комплексное изучение установленных норм и правил в конкретной прикладной области всегда является обязательным элементом культуры работающего в этой области специалиста.

#### **4. Ход работы:**

1. В соответствии с предложенным вариантом организации или предприятия проанализировать организационно-правовое обеспечение защиты информации в системе деятельности предприятия в целом.

- Государственная организация
  - Образование
  - Здравоохранение
  - другие
- Частная организация

2. Выявить существующие проблемные моменты и узкие места.

3. В соответствии с Законом "Об информации, информатизации и защите информации", Законом Российской Федерации "О безопасности" описать основные подходы к разработке организационно-правового обеспечения службы защиты информации на выбранном предприятии.

4. Определить круг задач службы защиты информации (СЗИ).

5. Сформулировать основные функции СЗИ.

6. Выделить в организационно-штатной структуре штатные единицы, обеспечивающие реализацию данных функции и особенности взаимодействия между собой.

7. Проанализировать нормативное обеспечение деятельности СЗИ, выявить проблемы.

8. Сформировать общую структуру нормативной документации по обеспечению безопасности информации в организации в следующей иерархии:

- Документы концептуального уровня, которые должны быть разработаны руководителями организаций;
- Документы общего уровня (применения);
- Документы, регламентирующие работу персонала с защищаемыми носителями.

9. Разработать отсутствующие документы, опираясь на законодательную базу, указанную в списке литературы, а также, используя Гарант, Консультант-Плюс. Доработать несоответствующие требованиям законодательства документы.

Разработать:

- 1) Положение о подразделении по защите информации. Общее руководство по руководству, функциям, задачам, правам, обязанностям, ответственности и штатной структуре.
- 2) Положение о перечне ресурсов.

### **5. Вопросы**

1. Какие функции выполняет СЗИ предприятия для решения задач защиты информации?
2. Как строится структура полномасштабной системы обеспечения безопасности и защиты информации предприятия?
3. Какова специфика организации и выполнения охранных функций?
4. Каковы суть и содержание нормативной основы организации ЗСИ?
5. Какие факторы влияют на формирование организационно-правового обеспечения защиты информации?
6. Какова структура организационно-правовой основы защиты информации?
7. Опишите организационно-правовые мероприятия по защите конфиденциальной информации.

### **Список дополнительной литературы:**

1. Справочно-поисковая система «Консультант Плюс»;
2. Справочно-поисковая система «Гарант»

## ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННЫХ РЕСУРСОВ

1. Ипатова, Э. Р. Методологии и технологии системного проектирования информационных систем : учебник / Э. Р. Ипатова, Ю. В. Ипатов. – 3-е изд., стер. – Москва : ФЛИНТА, 2021. – 256 с. – URL: <https://biblioclub.ru/index.php?page=book&id=79551> (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.
2. Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. – URL: <https://biblioclub.ru/index.php?page=book&id=598988> (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.
3. Аверченков, В. И. История развития системы государственной безопасности России : учебное пособие / В. И. Аверченков, В. В. Ерохин, О. М. Голембиовская ; науч. ред. Ю. Т. Трифанков. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 193 с. – URL: <https://biblioclub.ru/index.php?page=book&id=93267> (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.
4. Алдохина, О. И. Информационно-аналитические системы и сети : учебное пособие / О. И. Алдохина, О. Г. Басалаева. – Кемерово : КемГУКИ, 2010. – Часть 1. Информационно-аналитические системы. – 148 с. – URL: <https://biblioclub.ru/index.php?page=book&id=227684> (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.
5. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 255 с. – URL: <https://biblioclub.ru/index.php?page=book&id=276557> (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.