

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«Национальный исследовательский ядерный университет «МИФИ»

**Димитровградский инженерно-технологический институт –**

филиал федерального государственного автономного образовательного учреждения высшего образования  
«Национальный исследовательский ядерный университет «МИФИ»

**(ДИТИ НИЯУ МИФИ)**

**УТВЕРЖДАЮ**

Руководитель ДИТИ НИЯУ МИФИ  
*должность и название образовательного учреждения*

  
И.И. Бегина

« 12 » мая 20 21 г.

М.П.

**УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС**

**ПО УЧЕБНОЙ ДИСЦИПЛИНЕ**

ОП.01 Основы информационной безопасности

*Шифр, название дисциплины*

программы подготовки специалистов среднего звена по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

*Код, наименование специальности*

Форма обучения очная

Учебный цикл ОП

Составитель: Н.А. Шульга, преподаватель техникума ДИТИ НИЯУ МИФИ  
*ФИО, должность*

Димитровград 2021

УМК составлен на основе ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Минобрнауки РФ от 9 декабря 2016 г. № 1553 и ПООП, разработанной ФУМО в системе СПО по укрупненной группе специальностей 10.00.00 «Информационная безопасность», зарегистрированной в федеральном реестре примерных основных образовательных программ, регистрационный № 10.02.05-170703 от 03/07/2017 (Протокол № 1 от 28.03.2017)

Рассмотрен  
на заседании методической цикловой комиссии  
Информационных технологий  
Протокол № 8 от 26.03 2021 г.  
Председатель МЦК Г.М. Глек

## СОДЕРЖАНИЕ

Рабочая программа дисциплины (модуля)

ПРИЛОЖЕНИЕ 1 Аннотация

ПРИЛОЖЕНИЕ 2 Календарно-тематический план учебной дисциплины (модуля)

ПРИЛОЖЕНИЕ 3 Методические рекомендации по выполнению практических и/или лабораторных работ (инструкционные карты)

ПРИЛОЖЕНИЕ 4 Методические рекомендации по применению инновационных образовательных технологий и методов обучения в преподавании учебной дисциплины

ПРИЛОЖЕНИЕ 5 Методические рекомендации по организации самостоятельной работы

ПРИЛОЖЕНИЕ 6 Фонд оценочных средств (контрольно-измерительные материалы для учебной дисциплины, контрольно-оценочные средства для модуля)

ПРИЛОЖЕНИЕ 7 Лист регистрации дополнений и изменений УМК дисциплины (модуля)

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«Национальный исследовательский ядерный университет «МИФИ»

**Димитровградский инженерно-технологический институт -**  
филиал федерального государственного автономного образовательного учреждения высшего  
образования «Национальный исследовательский ядерный университет «МИФИ»  
(ДИТИ НИЯУ МИФИ)



УТВЕРЖДАЮ

Директор техникума ДИТИ НИЯУ МИФИ

*Н.А. Домнина* Н.А. Домнина

*15 апреля* 2021 г.

## РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.01 Основы информационной безопасности

Шифр, название дисциплины

программы подготовки специалистов среднего звена по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем


Код, наименование специальности

Форма обучения очная

Учебный цикл ОП

Составитель: Н.А. Шульга, преподаватель техникума ДИТИ НИЯУ МИФИ  
ФИО, должность

Программа составлена на основе ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Минобрнауки РФ от 9 декабря 2016 г. № 1553 и ПООП, разработанной ФУМО в системе СПО по укрупненной группе специальностей 10.00.00 «Информационная безопасность», зарегистрированной в федеральном реестре примерных основных образовательных программ, регистрационный № 10.02.05-170703 от 03/07/2017 (Протокол № 1 от 28.03.2017)

Рассмотрена  
на заседании методической цикловой комиссии  
Информационных технологий  
Протокол № 8 от 26.03 2021 г.  
Председатель МЦК  /Г.М. Глек/

## **СОДЕРЖАНИЕ**

<b>1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>4</b>
<b>2. СТРУКТУРА ПРИМЕРНОЙ УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>6</b>
<b>3. ПРИМЕРНЫЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ</b>	<b>10</b>
<b>4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ КОМПЕТЕНЦИЙ</b>	<b>12</b>
<b>5. ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ПРОГРАММЫ В ДРУГИХ ПООП</b>	<b>16</b>

# **1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**

## **1.1. Область применения примерной программы**

Примерная программа учебной дисциплины является частью примерной основной образовательной программы подготовки специалистов среднего звена (ППССЗ) в соответствии с ФГОС СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

## **1.2. Место дисциплины в структуре основной профессиональной образовательной программы подготовки специалистов среднего звена (ППССЗ):**

Учебная дисциплина ОП.01 Основы информационной безопасности по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем относится к обязательной части ППССЗ и входит в профессиональный цикл, ОП.00 Общепрофессиональные дисциплины.

Дисциплина ОП.01 Основы информационной безопасности входит в общепрофессиональный цикл, является дисциплиной, дающей начальные представления и понятия в области информационной безопасности, определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному самоопределению и самореализации в учебной деятельности.

## **1.3. Цель и планируемые результаты освоения дисциплины:**

В результате освоения дисциплины обучающийся должен **уметь**:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации;

В результате освоения дисциплины обучающийся должен **знать**:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;
- основные методики анализа угроз и рисков информационной безопасности;

В результате освоения дисциплины обучающийся осваивает элементы компетенций:

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

В14. Формирование глубокого понимания социальной роли профессии, позитивной и активной установки на ценности избранной специальности, ответственного отношения к профессиональной деятельности, труду.

В15. Формирование психологической готовности к профессиональной деятельности по избранной профессии.

В16. Формирование культуры исследовательской и инженерной деятельности

#### **1.4. Количество часов на освоение программы дисциплины:**

Объём образовательной нагрузки – 79 часов, в том числе:

- обязательная аудиторная нагрузка обучающегося - 60 часов;
- самостоятельная работа обучающегося - 4 часа;
- консультации – 4 часа;

Промежуточная аттестация установлена в форме экзамена (11ч.) в 4 семестре.



## 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

### 2.1. Объем учебной дисциплины и виды учебной работы

<b>Вид учебной работы</b>	<b>Объем часов</b>
<b>Объем образовательной нагрузки</b>	<b>79</b>
<b>- всего занятий</b>	<b>60</b>
<b>в том числе:</b>	
<b>теоретической обучение</b>	<b>30</b>
<b>практические занятия</b>	<b>30</b>
<b>самостоятельная учебная работа</b>	<b>4</b>
<b>консультации</b>	<b>4</b>
<b>Промежуточная аттестация (ЭКЗАМЕН в 4 семестре)</b>	<b>11</b>

## 2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объём часов	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4	5
<b>Раздел 1. Теоретические основы информационной безопасности</b>				
<b>Тема 1.1. Основные понятия и задачи информационной безопасности</b>	<b>Содержание учебного материала</b>	4	1	ОК 03. ОК 06. ОК 09. ПК 2.4 В14 В16
	Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от не информированности в области информационной безопасности.			
<b>Тема 1.2. Основы защиты информации</b>	<b>Содержание учебного материала</b>	12  6	2	ОК 03. ОК 06. ОК 09. ПК 2.4 В15
	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.			
	<b>Практические работы:</b>			
	№ 1 Определение объектов защиты на типовом объекте информатизации.	6		

	№ 2 Классификация защищаемой информации по видам тайны и степеням конфиденциальности			
<b>Тема 1.3. Угрозы безопасности защищаемой информации.</b>	<b>Содержание учебного материала</b>	10	2	ОК 03. ОК 06. ОК 09. ПК 2.4 В14. В15.
	Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к информации Уязвимости. Методы оценки уязвимости информации	4		
	<b>Практические работы:</b> № 3 Определение угроз объекта информатизации и их классификация	6	3	
<b>Раздел 2. Методология защиты информации</b>				
<b>Тема 2.1. Методологические подходы к защите информации</b>	<b>Содержание учебного материала</b>	4	1,2	ОК 03. ОК 06. ОК 09. ПК 2.4 В16.
	Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации.			
<b>Тема 2.2. Нормативно правовое регулирование защиты информации</b>	<b>Содержание учебного материала.</b>	8	1,2	ОК 03. ОК 06. ОК 09. ПК 2.4 В16.
	Организационная структура системы защиты информации Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации.			
	Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации	4		
	<b>Практические работы:</b> № 4 Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	4	3	
<b>Тема 2.3. Защита информации в автоматизированных (информационных) системах</b>	<b>Содержание учебного материала</b>	14	3	ОК 03. ОК 06. ОК 09. ПК 2.4 В14. В15.
	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах			
	Программные и программно-аппаратные средства защиты информации Инженерная защита и техническая охрана объектов информатизации Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.			
	<b>Практические работы:</b>	10		

	№ 5 Выбор мер защиты информации для автоматизированного рабочего места			B15.
	<b>Самостоятельная работа обучающихся:</b> - подготовка реферата по теме раздела			
	<b>Всего:</b>	<b>60</b>		
	<b>Консультации</b>	<b>4</b>		
	<b>Самостоятельная работа</b>	<b>4</b>		
	<b>Промежуточная аттестация</b>	<b>11</b>		
	<b>ИТОГО Объем ОП</b>	<b>79</b>		

*Для характеристики уровня освоения учебного материала используются следующие обозначения:*

- 1 – ознакомительный (воспроизведение информации, узнавание (распознавание), объяснение ранее изученных объектов, свойств и т.п.);*
- 2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);*
- 3 – продуктивный (самостоятельное планирование и выполнение деятельности, решение проблемных задач).*

### **3. ПРИМЕРНЫЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ**

#### **3.1. Материально-техническое обеспечение**

Реализация программы предполагает наличие учебного кабинета Информационных технологий, программирования баз данных

##### **Оборудование учебного кабинета:**

- Посадочные места по количеству обучающихся,
- доска,
- информационные стенды,
- стол компьютерный преподавателя,
- стол компьютерный студента,
- шкаф для документов,
- парта студенческая,

##### **Технические средства обучения:**

- проектор,
- интерактивная доска,
- принтер,
- системный блок,
- монитор,
- компьютер (1 системный блок + 2 монитора) – 8 шт,
- клавиатура,
- мышь,
- локальная сеть 100Мб/сек

#### **3.2. Информационное обеспечение обучения**

**Перечень используемых учебных изданий, Интернет-ресурсов, дополнительной литературы**

##### **Основная**

1. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. – М.: Академия. 2017. – 256 с.

##### **Дополнительные печатные источники**

2. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. – С-Пб.: Изд. Питер. 2017.

##### **Электронный ресурс**

3. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL:<https://urait.ru/bcode/475889>

4. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL:<https://urait.ru/bcode/475890>

Справочно-правовая система «Гарант» » [www.garant.ru](http://www.garant.ru)

Сайт Научной электронной библиотеки [www.elibrary.ru](http://www.elibrary.ru)

### 3.3. Методические рекомендации по организации изучения дисциплины

В целях реализации компетентностного подхода при преподавании дисциплины ОП.01 Основы информационной безопасности используются современные образовательные технологии: информационные технологии (компьютерные презентации), технологии развивающего обучения, технологии проблемного обучения (проблемное изложение, эвристическая беседа, исследовательский метод. В сочетании с внеаудиторной работой, для формирования и развития общих компетенций обучающихся применяются активные и интерактивные формы проведения занятий (групповая консультация, разбор конкретных ситуаций, групповая дискуссия).

Для проведения текущего контроля знаний и умений используется просмотр и оценка практических работ, выполненных учащимися на занятиях в аудитории и выполненных самостоятельно во внеаудиторное время.

## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ КОМПЕТЕНЦИЙ

Контроль и оценка результатов освоения компетенций осуществляется преподавателем в процессе проведения практических занятий, а также выполнения обучающимися индивидуальных заданий проектов исследований.

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
<b>Умения:</b> - классифицировать защищаемую информацию по видам тайны и степеням секретности; классифицировать основные угрозы безопасности информации;	Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий. Тестирование Экспертное наблюдение в процессе

**Знания:**

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;  
основные методики анализа угроз и рисков информационной безопасности.

практических занятий

## **АННОТАЦИЯ**

### **к рабочей программе учебной дисциплины ОП.01 Основы информационной безопасности по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем**

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена (ППССЗ) специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Рабочая программа составлена в соответствии с требованиями ФГОС СПО указанной специальности. В содержании рабочей программы отражены все дидактические единицы, указанные в образовательном стандарте, описаны цели и задачи дисциплины, место дисциплины в структуре ППССЗ, требования к результатам освоения дисциплины, объем дисциплины и виды учебной работы. Даны указания по учебно-методическому и информационному (перечень основной и дополнительной литературы, программного обеспечения, электронных образовательных ресурсов), материально-техническому обеспечению дисциплины.

В разделе «Контроль и оценка результатов освоения учебной дисциплины» описаны формы и методы входного, текущего контроля знаний и форма промежуточной аттестации студентов. Предусмотрены разнообразные формы организации самостоятельной работы студентов: написание рефератов, составление практических отчетов, решение профессиональных задач и т.д.

В рабочей программе указаны инновационные образовательные технологии, используемые при организации обучения по дисциплине.

Учебным планом по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем предусмотрен следующий объем учебной дисциплины: всего часов - 79, в том числе теория – 30 ч., практические занятия – 30 час., самостоятельная работа студентов - 4 час., консультации – 4ч. Вид промежуточной аттестации – (11ч.) экзамен в 4 семестре.

#### **Наименование разделов и тем дисциплины:**

#### **РАЗДЕЛ 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Тема 1.1. Основные понятия и задачи информационной безопасности

Тема 1.2. Основы защиты информации

Тема 1.3. Угрозы безопасности защищаемой информации.

#### **РАЗДЕЛ 2. МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ**

Тема 2.1. Методологические подходы к защите информации

Тема 2.2. Нормативно правовое регулирование защиты информации

Тема 2.3. Защита информации в автоматизированных (информационных) системах

**Разработчик рабочей программы:** Н.А. Шульга, преподаватель техникума ДИТИ НИЯУ МИФИ.



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«Национальный исследовательский ядерный университет «МИФИ»

**Димитровградский инженерно-технологический институт –**  
филиал федерального государственного автономного образовательного учреждения высшего  
образования «Национальный исследовательский ядерный университет «МИФИ»

**(ДИТИ НИЯУ МИФИ)**



УТВЕРЖДАЮ

Директор техникума ДИТИ НИЯУ МИФИ

Н.А. Домнина

15 апреля 2021 г.

## КАЛЕНДАРНО-ТЕМАТИЧЕСКИЙ ПЛАН

на 2021- 2022 уч. год,

Специальность: 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Дисциплина: **ОП.01 Основы информационной безопасности**

Курс, учебная группа: 2 курс, 241 гр.

Преподаватель: Н.А. Шульга

Общее количество часов на дисциплину - 79 час.

в том числе:

Самостоятельная работа – 4 ч.

Консультаций - 4 час.

Обязательных – 60ч, из них:

Теоретических занятий - 30 час.

Практических занятий - 30 час.

Промежуточная аттестация – 11 ч. (экз.)

Димитровград 2021

План составлен на основе ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Минобрнауки РФ от 9 декабря 2016 г. № 1553 и ПООП, разработанной ФУМО в системе СПО по укрупненной группе специальностей 10.00.00 «Информационная безопасность», зарегистрированной в федеральном реестре примерных основных образовательных программ, регистрационный № 10.02.05-170703 от 03/07/2017 (Протокол № 1 от 28.03.2017)

Рассмотрен  
на заседании методической цикловой комиссии  
Информационных технологий  
Протокол № 8 от 26.03 2021 г.  
Председатель МЦК Г.М. Глек /Г.М. Глек/

### Календарно-тематический план дисциплины

№ занятия	(ОК, ПК)	Наименование разделов и тем	Количество часов			Календарные сроки	Вид занятия	Учебно – методическое оснащение занятия	Учебная литература
			всего	ТЗ	ПЗ				
		<b>Раздел 1. Теоретические основы информационной безопасности</b>							
1.	ОК 03. ОК 06. ОК 09. ПК 2.4 В14. В15.	<b>Тема 1.1. Основные понятия и задачи информационной безопасности</b> Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.	2	2		Январь	урок	Лекция, презентация	Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. – М.: Академия. 2017. – 256 с.
2.	ОК 03. ОК 06. ОК 09. ПК 2.4 В16.	Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий.	2	2		Январь	урок	Лекция, презентация	Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. —

									342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <a href="https://urait.ru/bcode/475889">https://urait.ru/bcode/475889</a>
3.	ОК 03. ОК 06. ОК 09. ПК 2.4 В14. В15.	Сущность функционирования системы ЗИ. Защита человека от опасной информации и от не информированности в области информационной безопасности.	2	2		февраль	урок	Лекция, презентация	Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. – М.: Академия. 2017. – 256 с.
4.	ОК 03. ОК 06. ОК 09. ПК 2.4 В14. В15.	<b>Тема 1.2. Основы ЗИ</b> Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.	2	2		февраль	урок	Лекция, презентация	Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин,

									И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534- 10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <a href="https://urait.ru/bcode/475889">https://urait.ru/ bcode/475889</a>
5.	ОК 03. ОК 06. ОК 09. ПК 2.4 В14. В15.	Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи ЗИ. Основные понятия в области ЗИ	2	2		февраль	урок	Лекция, презентац ия	Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. – М.: Академия. 2017. – 256 с.
6.	ОК 03. ОК 06. ОК 09. ПК 2.4 В16.	Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.	2	2		февраль	урок	Лекция, презентац ия	Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие

									для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <a href="https://urait.ru/bcode/475889">https://urait.ru/bcode/475889</a>
7.	ОК 03. ОК 06. ОК 09. ПК 2.4 В14. В15.	№ 1 Определение объектов защиты на типовом объекте информатизации.	2		2	март	ПЗ	Инструкционная карта	Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. — М.: Академия. 2017. — 256 с.
8.	ОК 03. ОК 06. ОК 09. ПК 2.4 В14. В15.	№ 2 Определение объектов защиты на типовом объекте информатизации.	2		2	март	ПЗ	Инструкционная карта	
9.	ОК 03.	№ 3 Классификация защищаемой информации по	2		2	март	ПЗ	Инструк	

	ОК 06. ОК 09. ПК 2.4 В16.	видам тайны и степеням конфиденциальности						ионная карта	
10.	ОК 09. ОК 10. ПК 2.4. В16.	<p><b>Тема 1.3. Угрозы безопасности защищаемой информации.</b></p> <p>Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации.</p>	2	2		март	урок	Лекция, презентац ия	<p>Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534- 10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL:<a href="https://urait.ru/bcode/475889">https://urait.ru/ bcode/475889</a></p>

11.	ОК 09. ОК 10. ПК 2.4. В14. В15.	Каналы и методы несанкционированного доступа к информации Уязвимости. Методы оценки уязвимости информации	2	2		март	урок	Лекция, презентация	Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. – М.: Академия. 2017. – 256 с.
12.	ОК 09. ОК 10. ПК 2.4. В14. В15.	№ 4 Определение угроз объекта информатизации и их классификация	2		2	март	ПЗ	Инструкционная карта	Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. —
13.	ОК 09. ОК 10. ПК 2.4. В16.	№ 5 Определение угроз объекта информатизации и их классификация	2		2	апрель	ПЗ	Инструкционная карта	
14.	ОК 09. ОК 10. ПК 2.4.	№ 6 Определение угроз объекта информатизации и их классификация	2		2	апрель	ПЗ	Инструкционная карта	



									<a href="https://urait.ru/bcode/475889">URL:https://urait.ru/bcode/475889</a>
		<b>Раздел 2. Методология ЗИ</b>							
15.	ОК 09. ОК 10. ПК 2.4.	<b>Тема 2.1. Методологические подходы к защите информации</b> Анализ существующих методик определения требований к защите информации.	2	2		апрель	урок	Лекция, презентация	Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. – М.: Академия. 2017. – 256 с..
16.	ОК 09. ОК 10. ПК 2.4.	Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень ЗИ. Виды мер и основные принципы ЗИ	2	2		апрель	урок	Лекция, презентация	Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-

									10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <a href="https://urait.ru/bcode/475889">https://urait.ru/bcode/475889</a>
17.	ПК 2.4. В14. В15.	<b>Тема 2.2. Нормативно правовое регулирование ЗИ</b> Организационная структура системы ЗИ Законодательные акты в области ЗИ.	2	2		апрель	урок	Лекция, презентация	Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. – М.: Академия. 2017. – 256 с.
18.	ПК 2.4.	Российские и международные стандарты, определяющие требования к ЗИ. Система сертификации РФ в области ЗИ. Основные правила и документы системы сертификации РФ в области ЗИ	2	2		май	урок	Лекция, презентация	Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. —

									342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <a href="https://urait.ru/bcode/475889">https://urait.ru/bcode/475889</a>
19.	ПК 2.4.	№ 7 Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	2		2	май	ПЗ	Инструкционная карта	Бабаш А.В. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. – М.: Академия. 2017. – 256 с.
20.	ПК 2.4. В14. В15.	№ 8 Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	2		2	май	ПЗ	Инструкционная карта	Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования /
21.	ПК 2.4.	№ 9 Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	2		2	май	ПЗ	Инструкционная карта	
22.	ПК 2.4. В16.	№ 10 Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	2		2	май	ПЗ	Инструкционная карта	

									О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534- 10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <a href="https://urait.ru/bcode/475889">https://urait.ru/ bcode/475889</a>
23.	ОК 10. ПК 2.4.	<b>Тема 2.3. Защита информации в</b> Автоматизированных (информационных) системах Основные механизмы ЗИ. Система ЗИ. Меры ЗИ, реализуемые в автоматизированных (информационных) системах	2	2		май	урок	Лекция, презентац ия	Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. – М.: Академия. 2017. – 256 с.
24.	ОК 10. ПК 2.4.	Программные и программно-аппаратные средства ЗИ Инженерная защита и техническая охрана объектов информатизации Организационно- распорядительная ЗИ. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно -распорядительной системы.	2	2		май	урок	Лекция, презентац ия	Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения :

									учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <a href="https://urait.ru/bcode/475889">https://urait.ru/bcode/475889</a>
25.	ОК 10. ПК 2.4. В14. В15.	№ 11 Выбор мер ЗИ для автоматизированного рабочего места	2		2	июнь	ПЗ	Инструкционная карта	Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. – М.: Академия. 2017. – 256 с.
26.	ОК 10. ПК 2.4.	№ 12 Выбор мер ЗИ для автоматизированного рабочего места	2		2	июнь	ПЗ	Инструкционная карта	
27.	ОК 10. ПК 2.4. В16.	№ 13 Выбор мер ЗИ для автоматизированного рабочего места	2		2	июнь	ПЗ	Инструкционная карта	
28.	ОК 03.	№ 14 Итоговое занятие. Проверочная работа	2		2	июнь	ПЗ	Инструкционная	

	ОК 06.							карта	
29.	ОК 09. ОК 10. ПК 2.4. В14. В15. В16.	№ 15 Итоговое занятие. Проверочная работа	2		2	июнь	ПЗ	Инструкционная карта	
		<b>Всего:</b>	<b>60</b>	<b>30</b>	<b>30</b>				
		<b>Консультации</b>	<b>4</b>						
		<b>Самостоятельная работа</b>	<b>4</b>						
		<b>Промежуточная аттестация</b>	<b>11</b>						
		<b>ИТОГО Объем ОП</b>	<b>79</b>						

Преподаватель: \_\_\_\_\_ Н.А.Шульга

Приложение 4

к рабочей программе дисциплины ОП.01 Основы информационной безопасности

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«Национальный исследовательский ядерный университет «МИФИ»  
**Димитровградский инженерно-технологический институт -**  
филиал федерального государственного автономного образовательного учреждения высшего  
образования «Национальный исследовательский ядерный университет «МИФИ»  
**(ДИТИ НИЯУ МИФИ)**



УТВЕРЖДАЮ

Директор техникума ДИТИ НИЯУ МИФИ

Н.А. Домнина

15 августа 2021 г.

**Методические рекомендации по выполнению практических и/или  
лабораторных работ (инструкционные карты)  
по дисциплине ОП.01 Основы информационной безопасности**

**специальности 10.02.05 Обеспечение информационной безопасности  
автоматизированных систем**

Составитель: Н.А.Шульга, преподаватель техникума ДИТИ НИЯУ МИФИ

Димитровград 2021

## СОДЕРЖАНИЕ

Введение

Практическая работа №1. Работа со справочно-поисковой системой

«КонсультантПлюс»

Практическая работа №2. Работа со справочно-поисковой системой «Гарант»

Практическая работа №3. Нормативные правовые акты в области информационной безопасности

Практическая работа №4. Нормативные методические документы в области защиты информации

Практическая работа №5. Понятийный аппарат направления «Информационная безопасность»

Практическая работа №6. Регламенты автоматизированных систем

Практическая работа №7. Реализация модели политики безопасности

Практическая работа №8. Построение частной модели угроз безопасности персональных данных при их обработке в информационной системе

Практическая работа №9. Правовые задачи защиты информации

Практическая работа № 10. Применение инверсионного метода для выявления уязвимостей информационной системы

Приложения

Приложение 1. Компетенция магистранта направления «Управление информационной безопасности в профессиональном образовании»

Приложение 2. Тесты для самопроверки

Приложение 3. Содержание концепции обеспечения информационной безопасности учреждения

Библиографический список



## **ВВЕДЕНИЕ**

Основы информационной безопасности является одной из базовой дисциплин в профессиональной подготовке направления «Обеспечение информационной безопасности автоматизированных систем».

При изучении дисциплины студенты формируют компетенции, необходимые для выполнения следующих видов деятельности:

- организация работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации (ФСБ РФ), Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК РФ);
- организация и выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;
- разработка проектов организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности; аудит информационной безопасности информационных систем и объектов информатизации.

Значимость дисциплины обусловлена применением полученных знаний в дальнейшей исследовательской работе, при подготовке и защите диплома, в будущей профессиональной деятельности.

**Цель дисциплины** - сформировать способность и готовность студента в применении нормативно-правовых актов в области информационной безопасности в учреждениях профессионального образования.

### **Основные задачи курса:**

- сформировать систему знаний об основах организационного и правового обеспечения информационной безопасности, о содержании основных нормативных правовых актов в области обеспечения информационной безопасности и нормативных методических документов ФСБ России и ФСТЭК России в области защиты информации;
- сформировать умение организации работы по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации.
- создать условия для получения опыта по разработке организационно-распорядительных документов в области информационной безопасности.

### **Компетенции, формируемые в результате освоения учебной дисциплины:**

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

В14. Формирование глубокого понимания социальной роли профессии, позитивной и активной установки на ценности избранной специальности, ответственного отношения к профессиональной деятельности, труду.

В15. Формирование психологической готовности к профессиональной деятельности по избранной профессии.

В16. Формирование культуры исследовательской и инженерной деятельности.

Студент в ходе освоения учебной дисциплины должен:

**знать:**

- сущность и понятие информационной безопасности, характеристику её составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды угроз информационной безопасности;
- основные положения комплексного подхода к защите информации;
- основные нормативные правовые акты в области информационной безопасности и защиты информации, нормативные методические документы ФСБ и ФСТЭК РФ в данной области;

**уметь:**

- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- разрабатывать проекты нормативных и организационно распорядительных документов, регламентирующих работу по защите информации.

**владеть**

- основами работы с нормативными правовыми актами;
- основами организации обеспечения режима конфиденциальности и управления деятельностью служб защиты информации на учреждении;
- опытом разработки проектов организационно-распорядительных документов для учреждений профессионального образования.

Для формирования профессиональных компетенций студенту необходимо предложить различные виды практических работ.

Практические занятия проводятся с целью закрепления и углубления теоретических знаний, полученных обучающимися на лекциях и в ходе самостоятельной работы.

Настоящее учебное пособие предназначено для проведения практических работ студентов направления «Обеспечение информационной безопасности автоматизированных систем».

## ПРАКТИЧЕСКАЯ РАБОТА №1. РАБОТА СО СПРАВОЧНО-ИНФОРМАЦИОННОЙ ПРАВОВОЙ СИСТЕМОЙ «КОНСУЛЬТАНТПЛЮС»

**Цель работы:** ознакомиться с функционалом справочно-поисковой системой, приобрести практические навыки работы с информационной правовой системой «КонсультантПлюс»,

**Методы и приемы:** лабораторная работа с использованием информационно-коммуникационных технологий, выполнение упражнений, частично-поисковый метод, самостоятельная работа.

**Ключевые слова:** справочно-поисковая система, реквизиты нормативных актов, карточка поиска, правовой навигатор, обзор законодательства.

### Краткие теоретические сведения

Справочная правовая система (СПС) «КонсультантПлюс» включает все законодательство РФ: от основополагающих документов до узкоотраслевых

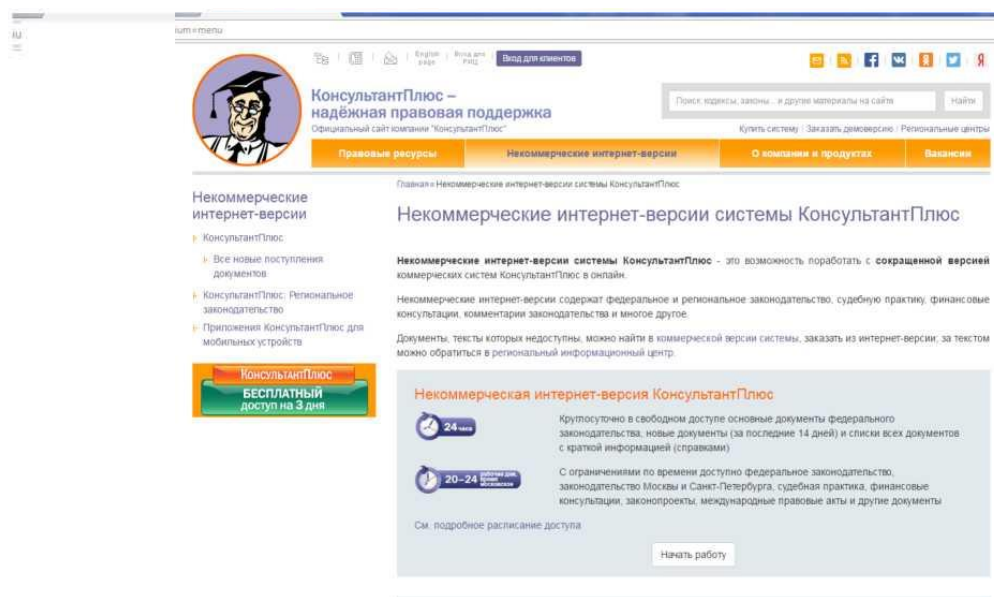


Рисунок 1. Стартовое окно СПС «КонсультантПлюс»

Некоммерческие интернет-версии СПС «КонсультантПлюс» содержат федеральное и региональное законодательство, судебную практику, финансовые консультации, комментарии законодательства, тематические обзоры.

Документы, тексты которых недоступны, можно найти в коммерческой версии системы, заказать из интернет-версии; за текстом можно обратиться в региональный информационный центр.

Для поиска необходимых документов, необходимо заполнить карточку поиска (рис.2).

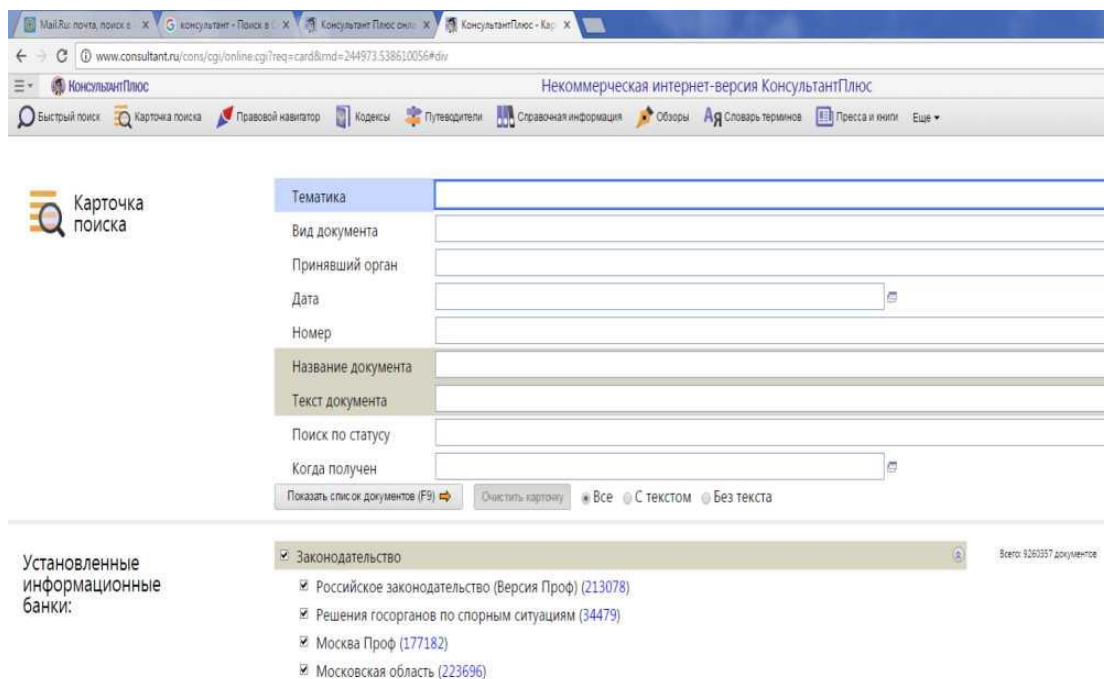


Рисунок 2. Карточка поиска некоммерческой интернет-версии КонсультантПлюс

Карточка поиска - основное средство поиска документов в базе данных системы. Система ищет документы, одновременно удовлетворяющие всем заполненным полям карточки поиска. Заполнять все поисковые поля не обязательно, достаточно заполнить лишь несколько полей.

В системе «КонсультантПлюс» предусмотрена возможность уточнять полученные списки несколько раз по разным полям.

Работа со справочно-правовой системой «КонсультантПлюс» сводится к следующему алгоритму:

- составление запроса на поиск документа или группы документов и их поиск;
- применение процедур обработки: сортировки, фильтрации и др.;
- использование механизма гиперссылок, поиска и создания папок и закладок при работе с текстом документа;
- чтение, редактирование, печать, сохранение текста документа в файл или экспорт данных в текстовый редактор MSWord или табличный редактор MSExcel.

На рисунке 3 представлен пример диалогового окна для тематического поиска документов.

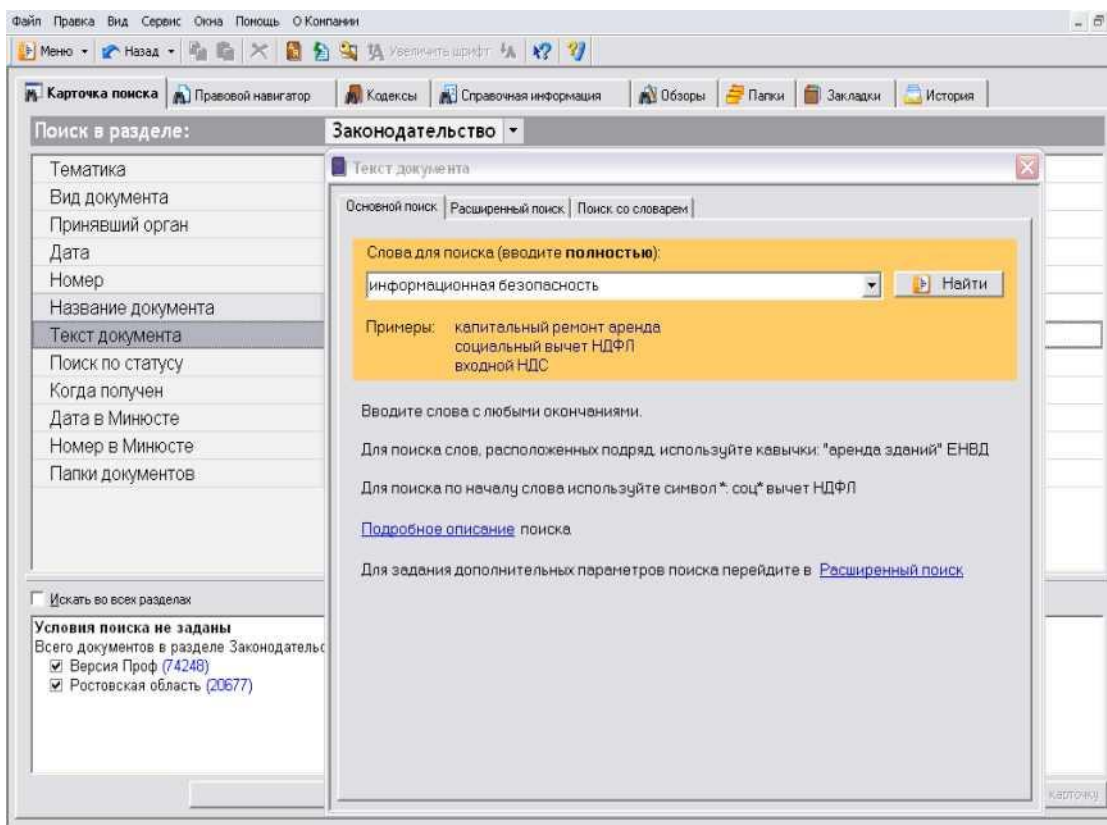


Рисунок 3. Окно поиска документа по правовому вопросу в системе «КонсультантПлюс»

### Порядок выполнения работы.

1. Открыть сайт: <http://www.consultant.ru>, выбрать вкладку работа с некоммерческими интернет-версиями
2. Ознакомиться с краткими теоретическими сведениями
3. Ознакомиться со структурой и возможностями некоммерческой интернет-версией СПС «КонсультантПлюс»
4. Открыть в новой вкладке MSWord, начать оформление отчета по лабораторной работе: записать тему, цель.
5. Войти из стартового окна в режим «Обзоры законодательства», просмотреть информацию в разделе: Правовые новости/ Специальный выпуск, вернуться в Стартовое окно.
6. Открыть по ссылке «Новые документы» списки документов, включенных в систему за последний месяц. Сохранить скриншот списка в отчет по лабораторной работе
7. Перейти в раздел «Законодательство», знакомиться с общим построением справочно-информационной правовой системы «КонсультантПлюс»
8. Изучить поочередно все подпункты основного меню системы, зайти в карточку поиска, рассмотреть все её элементы.
9. Зайти в режим Правового навигатора, изучить особенности поиска информации по конкретному правовому вопросу; двухуровневую структуру словаря; ключевые понятия и группы ключевых понятий; различные виды сортировки списка. Выйти из Правового навигатора.
10. Выполнить упражнения, указанные в таблице 1 - найти нормативноправовые документы, используя различные виды поиска
11. Ответить на контрольные вопросы.
12. Оформить отчет к лабораторной работе.

**Таблица 1. Упражнения для поиска нормативных документов в СПС «КонсультантПлюс».**

<b>Вид поиска</b>	<b>Задание</b>
Поиск по номеру и дате документа	Найдите Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Скопируйте реквизиты и преамбулу закона, вставьте эти данные в отчет по лабораторной работе. Найдите статью, посвященную ограниченному доступу к информации, скопируйте ее сохраните её в отчет.
Поиск по виду документа и его названию	Найдите основные документы по защите прав детей. Выделите три наиболее значимые, скопируйте реквизиты трех из них в отчет.
Поиск по правовому навигатору	Необходимо определить, чему равен минимальный размер оплаты труда (МРОТ). Найдите последний документ, которым внесены изменения в МРОТ. Вставьте его в отчет.
Поиск по принявшему органу	Найдите Приказ Генпрокуратуры РФ № 39 «О применении бланков процессуальных документов». Если документ отсутствует в некоммерческой интернет-версии, сделайте скриншот сервисного сообщения системы и вставьте его в отчет
Работа со списком документов	Сформируйте список документов о защите персональных данных. Поиск информации проводите по всем разделам справочной правовой системы. Список документов по данному вопросу сохраните в отчет.

#### **Контрольные вопросы**

1. Каковы основные разделы правовых документов в СПС «КонсультантПлюс»?
2. Что включается в иную официальную правовую информацию?
3. Перечислите основные инструменты поиска данной системы.
4. Как найти списки документов, регламентирующих конкретный правовой вопрос?
5. Из каких подразделов состоят разделы «Законодательство», «Судебная практика»?
6. В каком из разделов можно посмотреть тематические обзоры по проблемным правовым вопросам?
7. Как организована обратная связь с пользователями в данной системе?
8. Для чего применяется функция закладок в СПС «КонсультантПлюс»?

**Содержание отчета:** тема, цель, скриншоты основных этапов работы, результаты выполненных заданий, ответы на контрольные вопросы.

#### **Информационные источники:**

1. Фомичева Т.Г. Лабораторный практикум по курсу «Компьютерные технологии и в правовой практике» ЮжноРоссийский государственный технический университет, Новочеркасск, 2008
2. <http://www.consultant.ru>

## **ПРАКТИЧЕСКАЯ РАБОТА № 2: РАБОТА СО СПРАВОЧНО-ИНФОРМАЦИОННОЙ ПРАВОВОЙ СИСТЕМОЙ «ГАРАНТ»**

**Цель работы:** ознакомиться с функционалом и приобрести практические навыки работы со справочной правовой системой «Гарант», формировать устойчивые навыки самостоятельной работы.

**Методы и приемы:** лабораторная работа с использованием информационно-коммуникационных технологий, изучение алгоритмов, выполнение упражнений, частично-поисковый метод, самостоятельная работа.

**Ключевые слова:** справочно-поисковая система, реквизиты нормативных актов, сервисы справочно-правовой системы, обзор законодательства.

### **Краткие теоретические сведения**

Система производится в виде информационных блоков — баз данных, сформированных по тематическому принципу. Из информационных блоков формируется комплект, который и является конечным продуктом, предлагаемым заказчику. Ежедневное пополнение максимального комплекта составляет несколько десятков тысяч документов (включая документы судебной практики в виде онлайн-архива). Система включает все существующие виды правовой информации: акты органов власти федерального, регионального и муниципального уровня, судебную практику, международные договоры, проекты актов органов власти, формы (бухгалтерской, налоговой, статистической отчетности, бланки, типовые договоры), комментарии, словари и справочники. [википедия].

Работа со справочно-правовой системой «Гарант» начинается с организации поиска документа или списка документов.

Существуют следующие виды поиска в правовой системе «Гарант»: поиск по реквизитам, поиск по классификатору, поиск по ситуации, поиск по источнику опубликования, поиск по словарю терминов. Вид поиска выбирается в зависимости от того, какую информацию необходимо получить и какие имеются известные реквизиты.

Искомые слова можно вводить в любой из этих форм. Система самостоятельно переведет каждое введенное слово в нормальную форму. Однако, следует учесть, что слова необходимо вводить полностью, поскольку при сокращении система не может точно определить, для какого именно слова русского языка требуется подобрать грамматические формы.

Результатом поиска нескольких слов, словосочетаний или целых фраз будет список документов, включающих словоформы всех слов запроса. Документы, полученные таким образом, по умолчанию будут отсортированы особым образом - по степени соответствия.

При открытии документа, найденного с использованием поиска по тексту, искомые слова будут отмечены цветом, а сам документ откроется в месте, которое больше всего соответствует введенному контексту.

Сортировка *по степени соответствия* возможна только для списков, полученных при работе с *быстрым контекстным поиском*. Чем точнее конкретный документ соответствует содержанию запроса, тем выше его место в полученном списке.

Для получения изменений законодательства в определенной области в системе *существует индивидуальная новостная лента*. Она позволяет оперативно получить краткие тематические обзоры наиболее важных новых документов и судебных решений по интересующим вопросам [Фомичева].

### **Порядок выполнения работы**

1. Откройте сайт <http://www.garant.ru>, выберите интернет-версию ГАРАНТ.
2. Изучите краткие теоретические сведения.
3. Перейдите по ссылке «Помощь в работе, возможности системы».
4. Откройте страницу Информационно-обучающий видеокурс по работе с

интернет-версией системы ГАРАНТ (рис.4)

**Информационно-обучающий видеокурс по работе с интернет-версией системы ГАРАНТ "С системой ГАРАНТ Вы сможете больше!"**

'\*4

Уважаемый коллега!

Благодарим Вас за использование интернет-версии системы ГАРАНТ в Вашей работе!

В рамках представленного информационно-обучающего видеокурса Вы ознакомитесь с многообразием функциональных и аналитических возможностей системы ГАРАНТ и найдете



ответы на различные вопросы, которые могут возникнуть в процессе работы с системой. По окончании курса обучения предлагаем Вам проверить свои знания, ответив на вопросы итогового теста

Обратите внимание, кающему пользователю системы ГАРАНТ доступна удобная возможность индивидуального обучения, по результатам которого выдается именно Свидетельство. Помимо этого, Вы можете пройти дистанционное тестирование и получить Сертификат, подтверждающий уровень мастерства.

Желаем удачи в освоении возможностей ИПО ГАРАНТ и в изучении законодательства!

**Занятие 1** Главная страница системы ГАРАНТ

На первом занятии Вы узнаете о возможности выбрать свою профессиональную страницу в системе ГАРАНТ, научитесь быстро переходить к наиболее востребованной информации прямо с Главной страницы.

**Занятие 2** Поиск в системе ГАРАНТ

Занятие посвящено поисковым возможностям системы ГАРАНТ. Посмотрев его, Вы научитесь с легкостью выбирать оптимальный вид поиска необходимых материалов в системе и мгновенно находить их

**Занятие 3** Списки документов в системе ГАРАНТ

В процессе занятия Вы ознакомитесь с разнообразными инструментами системы ГАРАНТ, которые сделают просмотр и анализ списков документов еще более простым и удобным.

**Занятие 4** Изучение документа в системе ГАРАНТ

В ходе этого занятия Вы освоите ряд функциональных возможностей системы ГАРАНТ для работы с текстом документа: поиск контекста, установка закладок, изучение взаимосвязей документов, получение дополнительной информации и др

**Занятие 5** Анализ изменений нормы права

Занятие представляет возможности системы ГАРАНТ по изучению изменений, произошедших в документе. Вы научитесь сравнивать любые две редакции интересующего документа, находить текст документа, действовавший на определенную дату, узнавать об изменениях конкретного фрагмента.

**Занятие 6** Энциклопедии решений

В процессе занятия Вы узнаете об уникальных авторских материалах системы ГАРАНТ - Энциклопедиях решений, позволяющих легко разобраться в любых правовых ситуациях и быстро найти ответы на актуальные правовые вопросы.

**Занятие 7** Сервисы ГАРАНТа

Это занятие посвящено уникальным, доступным только пользователям системы ГАРАНТ возможностям. Вы узнаете, как

Рисунок 4. Страница с информационно-обучающим видеокурсом по СПС



## «Гарант»

5. Изучить возможности СПС «Гарант» с помощью видеокурсов занятий с 1 по 7
6. Пройти итоговый тест (рис.5). Продемонстрировать результат выполненного теста преподавателю
7. Найти нормативно-правовые документы из задания для самостоятельной работы, используя возможности СПС «Гарант». Составить краткий электронный конспект
8. Ответить на контрольные вопросы
9. Оформить отчет по лабораторной работе.

### ИТОГОВЫЙ ТЕСТ

#### к информационно-обучающему видеокурсу по работе с интернет-версией системы ГАРАНТ «С системой ГАРАНТ Вы сможете больше!»

Уважаемый коллега!

С помощью итогового теста Вы можете проверить свои знания интернет-версии системы ГАРАНТ.

Тест содержит 28 вопросов с предложенными ответами.

Вам нужно выбрать только один верный вариант из трех.

После ответа необходимо нажать кнопку «Принять».

Тест считается успешно пройденным, если дано не менее 75% верных ответов.

По окончании тестирования Вы сразу увидите итоговый результат.

Тестирование поможет Вам оценить уровень знаний и подскажет, какие уроки следует изучить еще раз.

Желаем удачи!

### Начать

Рисунок 5. Тест для диагностики знаний по функциональным возможностям СПС «ГАРАНТ»

#### Задания для самостоятельной работы

Составить электронный конспект по основным правовым актам в области информационной безопасности:

- ст. ст. 23, 24, 29, 42 Конституции РФ, ст. ст. 5,7,8,9 ФЗ "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (действующая редакция, 2016);
- ст.ст. 3, 4 Закона РФ от 27.12.1991 N 2124-1 (ред. от 03.07.2016) "О средствах массовой информации" (с изм. и доп., вступ. в силу с 15.07.2016),
- ст. ст. 7, 8, 9, 11 ФЗ "О персональных данных" от 27.07.2006 N 152-ФЗ (действующая редакция, 2016);
- сфера действия и принцип отнесения к гостайне ФЗ РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) "О государственной тайне";
- ст. 2 ФЗ "Об электронной подписи" от 06.04.2011 N 63-ФЗ (действующая редакция, 2016);
- ст.272, 273, 274 УК РФ.

#### Контрольные вопросы

1. Назовите виды поиска документов в СПС «Гарант».
2. Что такое быстрый контекстный поиск?
3. Назначение правового навигатора?
4. Какова структура единого информационного массива СПС «Гарант?»

5. Назовите элементы стартового окна СПС «Гарант?»
6. Как осуществляется переход к связанным документам?
7. Как просмотреть графические объекты?
8. Каков алгоритм работы с фильтрами в СПС «Гарант?»

**Содержание отчета:** Тема, цель, скриншоты основных этапов работы, электронный конспект, ответы на контрольные вопросы.

**Информационные источники:**

1. Фомичева Т.Г. Лабораторный практикум по курсу «Компьютерные технологии и в правовой практике» Южно-Российский государственный технический университет, Новочеркасск, 2008
2. <http://www.garant.ru>

**ПРАКТИЧЕСКАЯ РАБОТА №3: НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ**

**Цель:** ознакомиться с нормативными правовыми актами в области информационной безопасности, проанализировать систему действующих правовых актов РФ в области информационной безопасности, формировать устойчивые навыки самостоятельной работы.

**Методы и приемы:** лабораторная работа с использованием информационно-коммуникационных технологий, поисковая работа, анализ источников.

**Ключевые слова:** информационная безопасность, правовые акты, система нормативно-правовых актов.

**Порядок выполнения работы**

1. Используя любой интернет-браузер, найти правовые документы из представленного перечня.
2. Вставить недостающие реквизиты в перечень нормативных актов.
3. Составить аналитическую записку - обзор по предложенному перечню правовых актов.
4. Оформить отчет по лабораторной работе.

**Нормативно-правовые акты в области информационной безопасности РФ**

1. Конституция Российской Федерации, принята 12 декабря \_\_\_ г.
2. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О \_\_\_ отдельных видов деятельности».
3. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об \_\_\_ подписи».
4. Федеральный закон от 28 декабря 2010 г. № \_\_\_ -ФЗ «О безопасности».
5. Федеральный закон от 27 июля \_\_\_ г. № 152-ФЗ «О персональных данных».
6. Федеральный закон от 27 июля \_\_\_ г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
7. Федеральный закон от 19 декабря \_\_\_ г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
8. Федеральный закон от 7 июля \_\_\_ г. № 126-ФЗ «О связи».
9. Федеральный закон от 27 декабря \_\_\_ г. № 184-ФЗ «О техническом регулировании».
10. Закон РФ № 195-ФЗ от 30 декабря \_\_\_ г. «Кодекс Российской Федерации об административных правонарушениях».
11. Закон РФ № 63-ФЗ от 13 июня \_\_\_ г. «Уголовный кодекс Российской Федерации».
12. Закон РФ № 5485-1 от 21 июля \_\_\_ г. «О государственной тайне».

13. \_\_\_\_ национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации 31 декабря 2015 г. № 683.
14. \_\_\_\_ информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 5 декабря 2016 г. № 646.
15. Указ Президента Российской Федерации от 12 мая 2008 г. № \_\_\_\_ «Вопросы системы и структуры федеральных органов исполнительной власти».
16. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и \_\_\_\_ контролю».
17. Указ Президента Российской Федерации от 1 ноября 2008 г. № 1576 «О совете при Президенте Российской Федерации по развитию \_\_\_\_ общества в Российской Федерации».
18. Указ Президента Российской Федерации от 30 мая 2005 г. № \_\_\_\_ «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».
19. Указ Президента Российской Федерации от 17 марта 2008 г. № \_\_\_\_ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
20. Указ Президента Российской Федерации от 6 марта \_\_\_\_ г. № \_\_\_\_ «Об утверждении перечня сведений конфиденциального характера».
21. Концепция долгосрочного социально-экономического развития Российской Федерации на период до \_\_\_\_ года. Утверждена распоряжением Правительства Российской Федерации от 17 ноября 2008 г. № 1662-р.
22. Постановление Правительства Российской Федерации от 16 марта \_\_\_\_ г. № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».
23. Постановление Правительства Российской Федерации № \_\_\_\_ от 1 ноября 2012 г. «Об утверждении требований к защите \_\_\_\_ данных при их обработке в информационных системах персональных данных».
24. Постановление Правительства Российской Федерации от 6 июля 2008 г. № \_\_\_\_ «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
25. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № \_\_\_\_ «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
26. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № \_\_\_\_ «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
27. Постановление Правительства Российской Федерации от 21 марта 2012 г. № \_\_\_\_ «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
28. Постановление Правительства Российской Федерации от 18 сентября 2012 г. № \_\_\_\_ «Об утверждении правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с

федеральной службой безопасности российской федерации и федеральной службой по техническому и экспортному контролю».

29. Постановление Правительства Российской Федерации от 21 ноября 2011 г. № \_\_\_\_ «Об организации лицензирования отдельных видов деятельности».

30. Постановление Правительства Российской Федерации от 16 апреля 2012 г. № \_\_\_\_ «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

31. Постановление Правительства Российской Федерации от 3 февраля 2012 г. № \_\_\_\_ «О лицензировании деятельности по технической защите конфиденциальной информации».

32. Постановление Правительства Российской Федерации от 3 марта 2012 г. № \_\_\_\_ «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

33. Постановление Правительства РФ от 28 ноября 2011 г. № \_\_\_\_ «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи».

34. Постановление Правительства РФ от 09 февраля 2012 г. № \_\_\_\_ «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи».

35. Постановление Правительства Российской Федерации от 26 июня 1995 г. № \_\_\_\_ «О сертификации средств защиты информации».

#### **Контрольные вопросы:**

1. Какой документ из перечня является высшим в иерархии правовых актов?
2. Составьте иерархическую структуру нормативно-правовых актов РФ в области информационной безопасности, используя возможности MSWord
3. В каких случаях принимается Указ Президента?
4. В составленном перечне отметьте правовые акты, регламентирующие технические условия?
5. В составленном перечне отметьте правовые акты, регламентирующие организационные условия?
6. Какие документы из представленного перечня являются следствием ассоциирования правовых актов РФ с международным законодательством?

**Аналитическая записка** должна содержать иерархическую структуру исследованных правовых актов, сферу действия отдельных групп документов, соотношение и согласование групп правовых актов.

**Содержание отчета:** Тема, цель, перечень нормативно-правовых актов с полными реквизитами, ответы на контрольные вопросы, аналитическая записка.

1. <http://www.consultant.ru/>
2. <http://www.garant.ru/>
3. <http://www.e-nigma.ru/articles/>

**Информационные источники:**

**ПРАКТИЧЕСКАЯ РАБОТА №4: НОРМАТИВНЫЕ МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ.**

**Цель:** ознакомиться с нормативными методическими документами в области защиты информации, систематизировать сведения о нормативнометодических документах, приобрести опыт самостоятельного поиска и анализа.

**Методы и приемы:** лабораторная работа с использованием информационно-коммуникационных технологий, поисковая работа, анализ источников.

**Ключевые слова:** информационная безопасность, правовые акты, система нормативно-методических документов.

**Порядок выполнения работы.**

5. Используя любой интернет-браузер, найти нормативнометодические документы из представленного перечня.
6. Вставить недостающие реквизиты в перечень нормативных методических документов
7. Составить аналитическую записку - обзор по предложенному перечню.
8. Оформить отчет по лабораторной работе.

**Нормативно методические документы в области информационной безопасности РФ**

1. «Ответ требования и рекомендации по технической защите конфиденциальной информации» (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
2. «Сборник временных методик оценки защищенности конфиденциальной информации от утечки по Ответ каналам». Гостехкомиссия России. - М., 2002.
3. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические \_\_\_\_ . Госстандарт России. - М., 1995.
4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие \_\_\_\_ . Госстандарт России. - М., 2006.
5. ГОСТ Р 50922-2006. Защита информации. Основные термины и \_\_\_\_ - М., 2006.
6. ГОСТ Р ИСО/МЭК 15408-1- \_\_\_\_ . Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
7. ГОСТ Р ИСО/МЭК 15408-2- \_\_\_\_ . Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. Росстандарт России. - М., 2013.
8. ГОСТ Р ИСО/МЭК 15408-3- \_\_\_\_ . Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.
9. ГОСТ Р ИСО/МЭК \_\_\_\_ -2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий

обзор и терминология».

10. ГОСТ Р ИСО/МЭК 27001-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».
11. ГОСТ Р ИСО/МЭК 27002-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности», введен в действие с 01.01.2014
12. ГОСТ Р ИСО/МЭК 27003-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности».
13. ГОСТ Р ИСО/МЭК 27004-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения».
14. ГОСТ Р ИСО/МЭК 27005-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».
15. ГОСТ Р ИСО/МЭК 27006-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».
16. ГОСТ Р ИСО/МЭК 27011-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002».
17. ГОСТ Р ИСО/МЭК 27031-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса».
18. ГОСТ Р ИСО/МЭК 27033-1-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции».
19. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки \_\_\_\_. Защита криптографическая. Алгоритм криптографического преобразования.
20. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. \_\_\_ защита информации. Процессы формирования и проверки электронной цифровой подписи.
21. ГОСТ Р 34.10-\_\_\_ . Государственный стандарт Российской Федерации. Информационная технология. \_\_\_ защита информации. Процессы формирования и проверки электронной цифровой подписи.
22. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция \_\_\_ .
23. ГОСТ Р 34.11-\_\_\_ . Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция \_\_\_ .
24. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № \_\_\_ «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
25. Приказ ФСБ России от 9 февраля 2005 г. № \_\_\_ «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
26. Приказ ФСБ России от 30 августа 2012 г. № \_\_\_ «Об утверждении административного регламента Федеральной службы безопасности Российской Федерации

по предоставлению государственной услуги по осуществлению лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

27. Приказ \_\_\_ России от 08 августа 2009 г. № 149/7/2/6-1173 «Об утверждении типового регламента проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством РФ, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

28. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в \_\_\_ системах персональных данных с использованием средств автоматизации».

Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54144.

29. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих \_\_\_ тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622.

30. Приказ ФСБ России от 27 декабря 2011 г. № \_\_\_ «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

31. Приказ ФСБ России от 27 декабря 2011 г. № \_\_\_ «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».

32. Приказ ФСБ России от \_\_\_ июля \_\_\_ г. № \_\_\_ «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».

33. Приказ \_\_\_ России от 20 марта 2012 г. № \_\_\_ «Об утверждении требований к средствам антивирусной защиты».

34. Приказ \_\_\_ России от 6 декабря 2011 г. № \_\_\_ «Об утверждении требований к системам обнаружения вторжений».

35. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по \_\_\_ персональных данных».

36. Приказ Минкомсвязи России от 29 сентября 2011 г. № 242 «Об утверждении порядка передачи реестров квалифицированных сертификатов ключей проверки \_\_\_ подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования \_\_\_ подписи в случае прекращения деятельности аккредитованного удостоверяющего центра».

37. Приказ Минкомсвязи России от 23 ноября 2011 г. № \_\_\_ «Об утверждении

Административного регламента предоставления Министерством связи и массовых коммуникаций Российской Федерации государственной услуги по организации ведения единого государственного реестра сертификатов ключей подписей удостоверяющих центров, обеспечению доступа к нему и к реестру сертификатов ключей подписей уполномоченных лиц федеральных органов государственной власти, физических лиц и организаций».

38. Приказ Минкомсвязи России от 27 октября 2011 г. № \_\_\_ «Об утверждении Положения о Департаменте государственной политики в области создания и развития электронного правительства Министерства связи и массовых коммуникаций Российской Федерации».

39. Приказ Минкомсвязи России от 05 октября 2011 г. № \_\_\_ «Об утверждении порядка формирования и ведения реестров квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров».

40. Приказ Минкомсвязи России от 23 ноября 2011 г. № \_\_\_ «Об аккредитации удостоверяющих центров».

41. Приказ Минкомсвязи России от 13 апреля 2012 г. № \_\_\_ «Об обеспечении осуществления Министерством связи и массовых коммуникаций РФ функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров».

42. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть \_\_\_. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия \_\_\_ возможностей». - М., 1999.

43. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. \_\_\_ и определения». - М., 1992.

44. Руководящий документ Гостехкомиссии России «\_\_\_ защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». - М., 1992.

45. Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от \_\_\_ доступа к информации. Классификация автоматизированных систем и требования по защите информации». - М., 1992.

46. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Защита от \_\_\_ доступа к информации. Показатели защищенности от несанкционированного доступа к информации». - М., 1992.

47. Руководящий документ Гостехкомиссии России «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в \_\_\_ системах и средствах вычислительной техники». - М., 1992.

48. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. \_\_\_ экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». - М., 1997.

49. «Базовая модель угроз безопасности персональных данных при их обработке в \_\_\_ системах персональных данных». ФСТЭК России. - М., \_\_\_ .

50. «Методика определения \_\_\_ угроз безопасности персональных данных при их обработке в информационных системах персональных данных». ФСТЭК России. - М., 2008.

51. Приказ ФСТЭК России от 18 февраля \_\_\_ г. № \_\_\_ «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

52. Приказ ФСТЭК России от 11 февраля \_\_\_ г. № \_\_\_ «Об утверждении Требований



о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

53. Приказ ФСТЭК России от 14 марта \_\_\_ г. № \_\_\_ «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».

54. Приказ \_\_\_ России от 12 июля 2012 г. № 83 «Об утверждении административного регламента федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации».

55. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14 ноября 2011 г. № \_\_\_ «Об утверждении административного регламента проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных».

#### **Контрольные вопросы**

1. В составленном перечне отметьте правовые документы, регламентирующие технические условия?
2. В составленном перечне отметьте правовые документы, регламентирующие организационные условия?
3. Какие документы из представленного перечня являются следствием ассоциирования правовых актов РФ с международным законодательством?
4. Составьте классификацию исследованных документов по органу, принявшему тот или иной документ. Признак принадлежности к классу отметьте в перечне специальным значком.
5. Какова доля документов, регламентирующих организацию работ по защите персональных данных?
6. Какова доля документов, регламентирующих организацию работ по обороту средств технической защиты?

**Аналитическая записка** должна содержать иерархическую структуру исследованных правовых актов, сферу действия отдельных групп документов, соотношение и согласование групп правовых документов, принадлежность к государственному органу.

**Содержание отчета:** Тема, цель, перечень нормативно-правовых документов с полными реквизитами, ответы на контрольные вопросы, аналитическая записка.

#### **Информационные источники:**

1. <http://www.consultant.ru/>
2. <http://www.garant.ru/>
3. <http://www.e-nigma.ru/articles/>
4. <http://fstec.ru/>
5. <http://www.iso27000.ru/zakonodatelstvo/normativnye-dokumenty-fstek-rossii>

## **ПРАКТИЧЕСКАЯ РАБОТА №5: ПОНЯТИЙНЫЙ АППАРАТ НАПРАВЛЕНИЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

**Цель:** изучить понятийный аппарат направления «Информационная безопасность», получить опыт анализа и нормативных актов, формировать устойчивые навыки самостоятельной работы.

**Методы и приемы:** изучение теоретических источников, частичнопоисковая работа, анализ, формулирование понятий.

**Ключевые слова:** информационная безопасность, персональные данные, информационная система, информация, коммерческая тайна, государственная тайна, информационно-коммуникационные технологии, защита информации.

### **Порядок выполнения работы**

1. Сопоставить предложенный перечень понятий с определениями, приведенными ниже.
2. Результат сопоставления оформить в виде пар чисел, где арабская цифра - ключевое понятие, а римская цифра - его определение
3. Составить отчет по практической работе.

#### **Часть 1.**

1. **Вирус (компьютерный, программный)**
2. **Информационная система общего пользования**
3. **Документированная информация**
4. **Аутентификация отправителя данных**
5. **Государственная тайна**
6. **Информационная система**
7. **Автоматизированная обработка персональных данных**
8. **Блокирование персональных данных**
9. **Автоматизированная система**
10. **Информация**
11. **Гриф секретности**
12. **Вредоносная программа**
13. **Доступ к информации**
14. **Информационно-телекоммуникационная сеть**
15. **Вспомогательные технические средства и системы**
16. **Защищаемая информация.**
17. **Безопасность персональных данных**

I. программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных

II. возможность получения информации и ее использования

III. технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники

IV. информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации

V. реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него

- VI. сведения (сообщения, данные) независимо от формы их представления
- VII. временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)
- VIII. зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель
- IX. подтверждение того, что отправитель полученных данных соответствует заявленному
- X. состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных
- XI. технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных
- XII. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации
- XIII. совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
- XIV. обработка персональных данных с помощью средств вычислительной техники
- XV. система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций
- XVI. исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения
- XVII. информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

## **Часть 2**

- 1. Ключ проверки электронной подписи**
- 2. Межсетевой экран**
- 3. Несанкционированный доступ**
- 4. Коммерческая тайна**
- 5. Информационные технологии**
- 6. Идентификация**
- 7. Источник безопасности персональных данных**
- 8. Ключ электронной подписи**
- 9. Конфиденциальность**
- 10. Информационная система персональных данных**
- 11. Контролируемая зона**
- 12. Корпоративная информационная система**
- 13. Накопитель информации**
- 14. Контрагент**

**15. Нарушитель безопасности персональных данных**

**16. Конрагент**

**17. Недекларированные возможности**

I. уникальная последовательность символов, предназначенная для создания электронной подписи

II. устройство, предназначенное для записи и (или) чтения информации на носитель информации. Устройство конструктивно может содержать в себе неотчуждаемый носитель информации, либо может быть предназначено для использования сменных носителей информации. Накопители подразделяются на встроенные (в конструктиве системного блока) и внешние (подсоединяемые через порт). Встроенные накопители подразделяются на съемные и несъемные

III. информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц

IV. физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке (в том числе техническими средствами) в информационных системах персональных данных

V. функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации

VI. процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов

VII. присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов

VIII. уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи)

IX. обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

X. обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания

XI. совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств

XII. пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание сторонних лиц, а также транспортных, технических и иных материальных средств

XIII. субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации

XIV. сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию

XV. доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных

XVI. режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную

коммерческую выгоду

XVII. локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

### **Часть 3**

- 1. Распространение информации**
- 2. Побочные электромагнитные излучения и наводки**
- 3. Правила разграничения доступа**
- 4. Оператор**
- 5. Пользователь ИСПДн**
- 6. Обезличивание персональных данных**
- 7. Предоставление информации**
- 8. Оператор**
- 9. Перехват информации**
- 10. Владелец информации**
- 11. Носитель информации**
- 12. Технические средства ИСПДн**
- 13. Оператор ИС**
- 14. Программная закладка**
- 15. Персональные данные**
- 16. Программное ( программно-математическое воздействие)**
- 17. Ресурс информационной системы**

I. действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц

II. именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы

III. действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

IV. гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных

V. несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ

VI. любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

VII. физический объект, предназначенный для хранения информации

VIII. электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания

IX. код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, заблокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) заблокировать аппаратные средства

X. действия, направленные на получение информации неопределенным кругом лиц

или передачу информации неопределенному кругу лиц

XI. лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования

XII. неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов

XIII. государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных

XIV. лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам

XV. средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации)

XVI. совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

XVII. действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

#### **Часть 4**

- 1. Технический канал утечки информации**
- 2. Целостность информации**
- 3. Уполномоченное оператором лицо**
- 4. Электронный документ**
- 5. Электронное сообщение**
- 6. Разглашение информации, составляющей коммерческую тайну**
- 7. Сайт в сети Интернет**
- 8. Уничтожение персональных данных**
- 9. Утечка информации по техническим каналам**
- 10. Субъект доступа**
- 11. Электронная подпись**
- 12. Средства вычислительной техники**
- 13. Система защиты персональных данных**
- 14. Трансграничная передача персональных данных**
- 15. Удостоверяющий центр**
- 16. Угрозы безопасности персональных данных.**

I. совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных

II. неконтролируемое распространение информации от носителя защищаемой

информации через физическую среду до технического средства, осуществляющего перехват информации

III. действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору

IV. комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в ИСПДн

V. информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

VI. действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных

VII. информация, переданная или полученная пользователем информационно-телекоммуникационной сети

VIII. способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения)

IX. лицо или процесс, действия которого регламентируются правилами разграничения доступа

X. документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах

XI. передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу

XII. совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет"

XIII. юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом

XIV. лицо, которому на основании договора оператор поручает обработку персональных данных

XV. совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем

XVI. совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Содержание отчета:** Тема, цель, ответы по тематическим частям в виде пар чисел, где арабская цифра - ключевое понятие, а римская цифра - его определение.

#### **Информационные источники**

1. Чубукова С.Г. Организационное и правовое обеспечение информационной безопасности. Учебник и практикум. Серия: Профессиональное образование. ISBN: 9785991676076, Юрайт, 2016

2. <http://www.e-nigma.ru/articles/>
3. <http://fstec.ru/>

## **ПРАКТИЧЕСКАЯ РАБОТА №6: РЕГЛАМЕНТЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

**Цель:** ознакомиться с классификацией и регламентами автоматизированных систем (АС) различного назначения, получить знания применимости регламентов для конкретных АС, формировать устойчивые навыки самостоятельной работы.

**Методы и приемы:** изучение теоретических источников, формулирование определений, частично-поисковая работа, анализ, семинарское занятие.

**Ключевые слова:** автоматизированные системы (АС), регламенты АС, объекты информатизации, информационная безопасность, персональные данные, информационная система, государственные информационные системы информация, информационно-коммуникационные технологии, защита информации, ФСТЭК РФ, ФАПСИ РФ, ФСБ.

### **Порядок выполнения работы**

1. Найти определения АС в соответствии с классификацией, принятой в действующей системе правовых актов и нормативно-методических документов.
2. Вставить определения вместо пропусков.
3. Отметить нормативные документы, регламентирующие функционирование конкретной АС в предлагаемом перечне нормативных документов.
4. Проверить правильность выполнения заданий путем совместного обсуждения и проверки.
5. Оценить участие каждого из обучающегося в практической работе и семинаре по образцу таблицы 2.

*система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами)*

Отметьте в списке 12 нормативных документов, которые относятся к данному объекту информатизации

- |  |
|--|
| <ol style="list-style-type: none"><li>1. 149-ФЗ от 27 июля 2006 г.</li><li>2. Указ Президента РФ от 17 марта 2008 г. № 351</li><li>3. Пост. Правительства РФ № 1119 от 1 ноября 2012 г.</li><li>4. Пост. Правительства РФ № 512 от 6 июля 2008 г.</li><li>5. Пост. Правительства РФ № 687 от 15 сентября 2008 г.</li><li>6. Пост. Правительства РФ № 1233 от 3 ноября 1994 г.</li><li>7. СТР-К</li><li>8. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты»</li><li>9. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений»</li><li>10. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»</li><li>11. РД Гостехкомиссии «Защита от несанкционированного доступа к информации.</li></ol> |
|--|



Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей», 1999

12. РД Гостехкомиссии «Защита от несанкционированного доступа к информации. Термины и определения», 1992

13. РД Гостехкомиссии «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», 1992

14. РД Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», 1992

15. РД Гостехкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1992

16. РД Гостехкомиссии «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники», 1992

17. РД Гостехкомиссии «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к

18. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006

19. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008

20. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

21. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

*система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны)*

Отметьте в списке 4 нормативных документа, которые относятся к данному объекту информатизации

1. 149-ФЗ от 27 июля 2006 г.
2. Указ Президента РФ от 17 марта 2008 г. № 351
3. Пост. Правительства РФ № 1119 от 1 ноября 2012 г.
4. Пост. Правительства РФ № 512 от 6 июля 2008 г.
5. Пост. Правительства РФ № 687 от 15 сентября 2008 г.
6. Пост. Правительства РФ № 1233 от 3 ноября 1994 г.
7. СТР-К
8. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты»
9. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений»
10. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»
11. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»
12. РД Гостехкомиссии «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей», 1999
13. РД Гостехкомиссии «Защита от несанкционированного доступа к РД Гостехкомиссии «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», 1992
14. РД Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», 1992
15. РД Гостехкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1992
16. РД Гостехкомиссии «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники», 1992
17. РД Гостехкомиссии «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1997

*автоматизированные системы управления, обеспечивающие контроль и управление технологическим и (или) производственным оборудованием (исполнительными устройствами) и реализованными на нем технологическими и (или) производственными процессами (в том числе системы диспетчерского управления, системы сбора (передачи) данных, системы, построенные на основе программируемых логических*

**контроллеров, распределенные системы управления, системы управления станками с числовым программным управлением).**

Отметьте в списке 6 нормативных документов, которые относятся к данному объекту информатизации

1. 152-ФЗ от 27 июля 2006 г.
2. 98-ФЗ от 29 июля 2004 г.
3. Пост. Правительства РФ № 1119 от 1 ноября 2012 г.
4. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты»
5. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений»
6. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»
7. РД Гостехкомиссии «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей», 1999
8. РД Гостехкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1992
9. РД Гостехкомиссии «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1997
10. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006
11. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
12. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
13. Приказ ФСТЭК России от 14 марта 2014 г. № 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»

***информационно-управляющая или информационно-коммуникационная система, которая осуществляет управление критически важным объектом (процессом), или информационное обеспечение управления таким объектом (процессом), или официальное информирование граждан и в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация или будут нарушены выполняемые системой функции управления со значительными негативными последствиями.***

Отметьте в списке 6 нормативных документов, которые относятся к данному объекту информатизации

1. 152-ФЗ от 27 июля 2006 г.
2. Пост. Правительства РФ № 1119 от 1 ноября 2012 г.
3. Пост. Правительства РФ № 1233 от 3 ноября 1994 г.
4. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты»

5. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений»
6. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»
7. РД Гостехкомиссии «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей», 1999
8. РД Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», 1992
9. РД Гостехкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1992
10. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры
11. Методика определения актуальных угроз безопасности информации

в ключевых системах информационной инфраструктуры

12. Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
13. Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры.
14. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008.
15. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006
16. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008
17. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
18. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
19. Приказ ФСТЭК России от 14 марта 2014 г. № 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»

***совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.***

Отметьте в списке 11 нормативных документов, которые относятся к данному объекту информатизации

1. 152-ФЗ от 27 июля 2006 г.
2. 149-ФЗ от 27 июля 2006 г.
3. Пост. Правительства РФ № 1119 от 1 ноября 2012 г.

4. Пост. Правительства РФ № 512 от 6 июля 2008 г.
5. Пост. Правительства РФ № 687 от 15 сентября 2008 г.
6. Пост. Правительства РФ № 1233 от 3 ноября 1994 г.
7. Пост. Правительства РФ № 211 от 21 марта 2012 г.
8. Пост. Правительства РФ № 953 от 24 ноября 2009 г.
9. СТР-К
10. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты»
11. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений»
12. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в

информационных системах общего пользования»

13. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»
14. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры
15. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры
16. Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
17. Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
18. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008
19. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006
20. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008
21. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
22. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
23. Приказ ФСТЭК России от 14 марта 2014 г. № 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»

***федеральные информационные системы и региональные информационные системы, созданные на основании соответственно Федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.***

Отметьте в списке 6 нормативных документов, которые относятся к данному объекту информатизации

1. 149-ФЗ от 27 июля 2006 г.
2. 98-ФЗ от 29 июля 2004 г.
3. Указ Президента РФ от 17 марта 2008 г. № 351
4. Пост. Правительства РФ № 1119 от 1 ноября 2012 г.
5. Пост. Правительства РФ № 1233 от 3 ноября 1994 г.
6. СТР-К
7. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты»
8. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений»
9. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»
10. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры
11. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры
12. Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
13. Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
14. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008
15. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006
16. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008
17. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
18. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
19. Приказ ФСТЭК России от 14 марта 2014 г. № 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»

***федеральные государственные информационные системы, созданные или используемые в целях реализации полномочий федеральных органов исполнительной***

**власти и содержащие сведения о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти, обязательных для размещения в информационно-телекоммуникационной сети Интернет, определяемые Правительством Российской Федерации.**

Отметьте в списке 2 нормативных документа, которые относятся к данному объекту информатизации

1. 98-ФЗ от 29 июля 2004 г.
2. Пост. Правительства РФ № 1119 от 1 ноября 2012 г.
3. Пост. Правительства РФ № 1233 от 3 ноября 1994 г.
4. Пост. Правительства РФ № 211 от 21 марта 2012 г.
5. Пост. Правительства РФ № 953 от 24 ноября 2009 г.
6. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»
7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008
8. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006
9. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008
10. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
11. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
12. Приказ ФСТЭК России от 14 марта 2014 г. № 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»

**Таблица 2 Образец чек-листа для взаимного оценивания**

Ф.И.О.	Степень участия: правильность выполнения, активность в обсуждении и приведении аргументов, баллы от 1 до 5

**Информационные источники:**

1. Чубукова С.Г. Организационное и правовое обеспечение информационной безопасности. Учебник и практикум. Серия: Профессиональное образование. ISBN: 9785991676076, Юрайт, 2020
2. <http://www.e-nigma.ru/articles/>
3. <http://fstec.ru/>

## ПРАКТИЧЕСКАЯ РАБОТА №7: РЕАЛИЗАЦИЯ МОДЕЛИ ПОЛИТИКИ БЕЗОПАСНОСТИ

**Цель:** ознакомиться с моделями управления доступом, научиться составлять матрицу доступа и иерархию ролей для учреждения профессионального учреждения для целей реализации политики безопасности, получить опыт принятия мотивированного решения.

**Методы и приемы:** изучение теоретических источников, контент-анализ сайтов образовательных учреждений, моделирование (политики безопасности), структурное программирование, кейс-метод.

**Ключевые слова:** политика безопасности, матрица доступа, ролевое управление доступом, мандатное управление доступом, объектно-ориентированный подход в ролевом управлении доступом, наследование ролей, инкапсуляция ролей

### Краткие теоретические сведения

Под политикой безопасности понимают набор норм, правил и практических приемов, регулирующих управление, защиту и распределение ценной информации.

Политика безопасности задает механизмы управления доступа к объекту, определяет как разрешенные, так и запрещенные доступы.

Политика безопасности реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Для конкретной организации политика безопасности должна носить индивидуальный характер и зависеть от конкретной технологии обработки информации и используемых программных и технических средств.

В ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах Гостехкомиссии РФ определены два вида (принципа) разграничения доступа: дискретное (дискреционное, избирательное) управление доступом; мандатное (полномочное) управление доступом.

**Избирательное (или дискреционное) управление доступом** характеризуется заданным администратором множеством разрешенных отношений доступа (например, в виде троек объект - субъект - тип доступа). Обычно для описания свойств избирательного управления доступом применяют математическую модель на основе матрицы доступа.

Матрица доступа представляет собой матрицу, в которой столбец соответствует объекту системы, а строка - субъекту.

На пересечении столбца и строки матрицы указывается тип разрешенного доступа субъекта к объекту.

Матрица доступа является самым простым подходом к моделированию систем управления доступом. С ростом организации, увеличивается опасность хищения информации, в том числе сотрудниками, возрастают финансовые и репутационные риски, это приводит к ужесточению политик и систем контроля. Любые избыточные права доступа сотрудников ведут к увеличению риска утечки информации, в связи с чем, происходит ужесточение политики ИБ, так как увеличиваются риски утечки информации.

Избирательная политика безопасности широко применяется в автоматизированных системах коммерческого сектора, так как её реализация соответствует требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость.

**Полномочная политика безопасности** основана на полномочном (мандатном) способе управления доступом. Полномочное (или мандатное) управление доступом характеризуется совокупностью правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от метки конфиденциальности информации и уровня допуска пользователя [5]. Полномочное управление доступом подразумевает, что:

- 1) все субъекты и объекты системы однозначно идентифицированы;



- 2) каждому объекту системы присвоена метка конфиденциальности информации, определяющая ценность содержащейся в нем информации;
- 3) каждому субъекту системы присвоен определенный уровень допуска, определяющий максимальное значение метки конфиденциальности информации объектов, к которым субъект имеет доступ.

Чем важнее объект, тем выше его метка конфиденциальности, поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки конфиденциальности.

Основное назначение полномочной политики безопасности - регулирование доступа субъектов системы к объектам с различными уровнями конфиденциальности, предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние.

При выборе и реализации политики безопасности в автоматизированной системе проводится анализ угроз и рисков для информации и информационного обмена и определяются правила использования для любого информационного процесса, права доступа к элементам информации с учетом данной оценки ценностей. Фрагмент матрицы доступа представлен в таблице 3.

**Таблица 3 Пример матрицы доступа**

Объект / Субъект	Файл_1	Файл_2	CD-RW	Дисковод
Администратор	Полные права	Полные права	Полные права	Полные права
Гость	Запрет	Чтение	Чтение	Запрет
Пользователь_1	Чтение, передача прав	Чтение, запись	Полные права	Запрет

### **Ролевое управление доступом**

При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования, так как число связей в них пропорционально произведению количества пользователей на количество объектов, и тогда в этом случае принимаются решения в объектно-ориентированном стиле, способные эту сложность понизить. Таким решением является **ролевое управление доступом**.

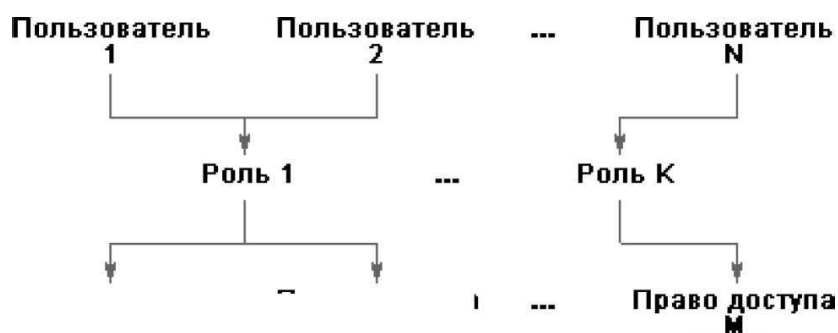
Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности - роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права (см. рис. 6). Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; его можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование, поскольку он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей, прежде всего за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах. Кроме того, ролей должно быть значительно меньше, чем пользователей. В результате число администрируемых связей становится пропорциональным сумме (а не произведению) количества пользователей и объектов, что по порядку величины уменьшить уже невозможно. Ролевое управление доступом оперирует следующими основными понятиями: **пользователь** (человек, интеллектуальный автономный агент и

т.п.); **сеанс работы пользователя**; **роль** (обычно определяется в соответствии с организационной структурой); **объект** (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД); **операция** (зависит от объекта; для файлов ОС - чтение, запись, выполнение и т.п.; для таблиц СУБД - вставка, удаление и т.п., для прикладных объектов операции могут быть более сложными); **право доступа** (разрешение выполнять определенные операции над определенными объектами).

### Право доступа Право доступа

#### 1 2

Ролям приписываются пользователи и права доступа, то есть реализуется отношения "многие ко многим" между пользователями и правами. Роли могут быть приписаны многим пользователям; один пользователь может быть приписан нескольким ролям. Во время сеанса работы пользователя активизируется подмножество ролей, которым он приписан, в результате чего он становится обладателем объединения прав, приписанных активным ролям. Одновременно пользователь может открыть несколько сеансов. Между ролями может быть определено отношение частичного порядка, называемое наследованием. Если роль r2 является наследницей r1, то все права r1 приписываются r2, а все пользователи r2 приписываются r1.



Очевидно, что **наследование ролей** соответствует наследованию классов в объектно-ориентированном программировании, только правам доступа соответствуют методы классов, а пользователям - объекты (экземпляры) классов. Отношение наследования является иерархическим, причем права доступа и пользователи распространяются по уровням иерархии навстречу друг другу. В общем случае наследование является множественным, то есть у одной роли может быть несколько предшественниц (и, естественно, несколько наследниц, которых мы будем называть также преемницами).

Можно представить формирование **иерархии ролей**, начиная с минимума прав (и максимума пользователей), приписываемых роли "сотрудник", с постепенным уточнением состава пользователей и добавлением прав (роли "системный администратор", "бухгалтер" и т.п.), до роли "руководитель".

При формировании иерархии ролей учитывается принцип **минимизации привилегий**, то есть каждой роли разрешено только то, что необходимо для выполнения служебных обязанностей.

### Порядок выполнения работы:

1. Изучить теоретические сведения
2. Найти сайт образовательного учреждения
3. Смоделировать политику безопасности образовательного учреждения и составить матрицу доступа для образовательного учреждения.
4. Составить иерархию ролей для данного образовательного учреждения с описанием ролей сотрудников. При описании должен быть реализован принцип минимизации

привилегий.

5. Ответить на контрольные вопросы. Оформить отчет.

**Контрольные вопросы**

1. Что понимается под политикой безопасности?
2. В чем заключается модель дискреционной политики безопасности?
3. В чем заключается модель мандатной политики безопасности?
4. Что понимается под матрицей доступа в дискреционной политике безопасности?  
Что хранится в данной матрице?
5. Как соотносятся матрица доступа и ролевой доступ?
6. В каких случаях целесообразно использовать ролевой доступ?
7. В чем состоит принцип минимизации привилегий?

**Содержание отчета:** Тема, цель, матрица доступа учреждения, ролевой доступ, ответы на контрольные вопросы.

**Информационные источники:**

1. Галатенко В.А. Идентификация и аутентификация, управление доступом [Электронный ресурс]:  
<http://citforum.ru/security/articles/galatenko/>- (дата обращения - 01.03.2017)
2. <https://www.anti-malware.ru/node/13626#part4>

## **ПРАКТИЧЕСКАЯ РАБОТА №8: ПОСТРОЕНИЕ ЧАСТНОЙ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ.**

**Цель:** ознакомиться с содержанием и структурой частной модели угроз безопасности в информационной системе персональных данных (ИСПДн), получить опыт создания частной модели угроз безопасности для учреждения, имеющего информационную систему обработки персональных данных.

**Методы и приемы:** изучение теоретических источников, анализ, работа по шаблону, проектный кейс-метод, частично-поисковая работа, самостоятельная работа.

**Ключевые слова:** частная модель угроз, персональные данные, информационная система, модель нарушителя, угрозы утечки информации, технические каналы утечки информации, защищенность информационной системы, вероятность реализации угроз, корпоративная сеть, несанкционированный доступ.

### **Порядок выполнения работы**

1. Изучить исходные условия существующей ИСПДн
2. Копировать шаблон частной модели угроз
3. Заполнить шаблон частной модели угроз по исходным условиям информационной систем обработки персональным данным.
4. Защитить свой проект частной модели угроз ИСПДн.

#### **Исходные условия ИСПДн «Кадры»**

**Организация:** ЗАО «Солнышко».

**Директор:** Иванов Иван Иванович.

**Заместитель директора:** Петрова Тамара Васильевна.

**Начальник отдела кадров:** Южина Мария Ивановна.

**Сотрудники отдела кадров:** Сидорова Александра Павловна,  
Копылова Юлия Фёдоровна.

#### **Состав ИСПДн:**

1. Персональные данные сотрудников организации:
  - фамилия, имя, отчество
  - дата и место рождения
  - пол
  - сведения об образовании
  - сведения о предыдущем месте работы
  - семейное положение
  - адреса регистрации и фактического проживания
  - номера контактных телефонов
  - индивидуальный номер налогоплательщика
  - номер страхового свидетельства пенсионного страхования
  - номер полиса обязательного медицинского страхования
  - данные водительского удостоверения

В информационной системе одновременно обрабатываются данные 777 субъектов персональных данных (сотрудников) в пределах Организации.

2. Три автоматизированных рабочих места (АРМ) пользователей, сетевой принтер, сервер, коммутационное оборудование.

**Топология:** АРМ и сервер составляют сегмент корпоративной вычислительной сети (см. схему - рис. 7).

**Корпоративная сеть:** Организации не имеет подключения к сетям связи общего пользования и сетям международного информационного обмена.

В состав каждого АРМ входят два жёстких диска, на первом установлена операционная система, прикладное программное обеспечение и общедоступная справочная

информация, на втором - информация, составляющая персональные данные сотрудников Организации.

Комплект АРМ №1-3: Системный блок № XXXXXXXX01-03, Монитор Samsung N710 - серийный номер YYYYYYYY01-03, клавиатура Genius серийный номер ZZZZZZZZ01-03, графический манипулятор (мышь) Genius серийный номер WWWW01-03,

В состав сервера входят три жестких диска, на первом установлена операционная система, прикладное программное обеспечение, второй и третий объединены в RAID массив, в котором хранится информация, составляющая персональные данные сотрудников Организации.

Комплект сервера: Системный блок № XXXXXXXX04, Монитор Samsung N710 - серийный номер YYYYYYYY04, клавиатура Genius серийный номер ZZZZZZZZ04, графический манипулятор Genius серийный номер WWWW04.

Сервер и коммуникационное оборудование установлены в типовой стойке.

Сетевой принтер HP LaserJet P2015 серийный номер SSSSSSSS.

### 3. Технология обработки персональных данных:

Обработка персональных данных сотрудников включает весь перечень действий.

К работе на АРМ допущены сотрудники отдела кадров и заместитель директора.

Полный доступ ко всей информации на АРМ и сервере имеют заместитель директора и начальник отдела кадров.

Сотрудники отдела кадров имеют полный доступ только к каталогу «Личные дела», размещённой на диске №2 своего АРМ, и только на чтение информации из каталога «Личные дела» на сервере.

Системный администратор сегмента сети не имеет доступа к информации, составляющей персональные данные. Имеет права на установку, настройку программного обеспечения, программных (программно-аппаратных) средств защиты сервера и АРМ № 1-3. Режим работы - одновременный.

**Расположение:** Отдельный кабинет по адресу: РФ, г. Отрадный, ул. Веселая,, дом 6, офис 25.

Помещение офиса оборудовано охранной сигнализацией и в нерабочее время сдаётся под охрану.

Доступ в помещение ограничен распорядительными актами Организации и автоматизированной системой контроля и управления доступа.

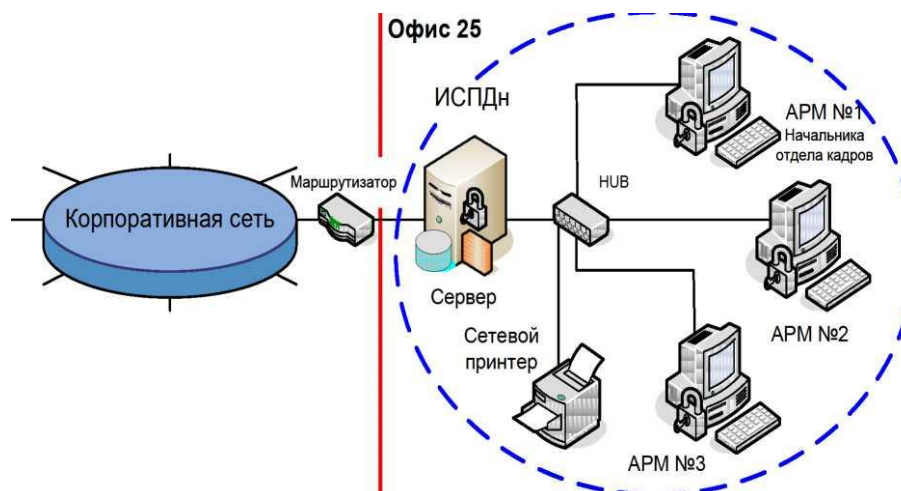


Рисунок 7. Схема корпоративной сети

**УТВЕРЖДАЮ**

*(должность руководителя  
организации)*

*(подпись)*

« \_\_\_\_ » \_\_\_\_\_ 201 \_\_\_\_ г.

**Частная модель угроз  
безопасности персональных данных  
при их обработке в ИСПДн**

\_\_\_\_\_  
*(наименование ИСПДн)*

**СОГЛАСОВАНО**

**СОГЛАСОВАНО**

« \_\_\_\_ » \_\_\_\_\_  
201 \_\_\_\_ г

« \_\_\_\_ » \_\_\_\_\_  
201 \_\_\_\_ г.

## **Сокращения, условные обозначения**

## **Термины и определения**

## **Введение.**

Современная система обеспечения информационной безопасности должна строиться на основе комплексирования разнообразных мер защиты и должна опираться на современные методы прогнозирования, анализа и моделирования возможных угроз безопасности информации и последствий их реализации.

Результаты моделирования предназначены для выбора адекватных оптимальных методов парирования угроз.

На стадии моделирования проведено изучение и анализ существующей обстановки и выявлены актуальные угрозы безопасности ПДн в составе ИСПДн

---

Модель угроз построена в соответствии с

### **1. Описание ИСПДн**

**1.1.** Описание условий создания и использования ПДн

**1.2.** Описание форм представления ПДн

**1.3.** Описание структуры ИСПДн

**1.4.** Описание характеристик безопасности

### **2. Описание подхода к моделированию угроз безопасности ПДн.**

Модель угроз безопасности ПДн в составе ИСПДн разработана на основе методических документов ФСТЭК:

На основе «Базовой модели угроз безопасности ПДн при их обработке в ИСПДн» проведена классификация угроз безопасности ПДн в составе ИСПДн и составлен перечень угроз безопасности ПДн в составе ИСПДн.

На основе составленного перечня угроз безопасности ПДн в составе ИСПДн с помощью «Методики определения актуальных угроз безопасности ПДн при их обработке в ИСПДн» построена модель угроз безопасности ПДн в составе ИСПДн и выявлены актуальные угрозы.

### **3. Классификация угроз безопасности персональных данных в ИСПДн**

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угроз.

К характеристикам ИСПДн, обуславливающим возникновение УБПДн, можно отнести:

ИСПДн представляет собой совокупность информационных и программно-аппаратных элементов и их особенностей как объектов обеспечения безопасности.

Основными элементами ИСПДн являются:

Основными элементами канала реализации УБПДн являются:

Носители ПДн могут содержать информацию, представленную в следующих видах:

В целях формирования систематизированного перечня УБПДн при их обработке в ИСПДн угрозы классифицируются в соответствии со следующими признаками:

Реализация одной из УБПДн перечисленных классов или их совокупности может привести к следующим **типам последствий** для субъектов ПДн:

Угрозы утечки ПДн по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и приемника информативного сигнала, то есть определяются характеристиками технического канала утечки ПДн и описываются следующим образом:

Угрозы, связанные с НСД, представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДн, способов реализации угроз, объектов воздействия (носителей защищаемой информации) и возможных деструктивных действий. Такое представление описывается

следующей формализованной записью:

### **3.1. Общее описание угроз безопасности ПДн, обрабатываемых в ИСПДн**

При обработке ПДн в ИСПДн возможна реализация следующих видов УБПДн:

### **3.2. Угрозы утечки информации по техническим каналам.**

Основными элементами угроз утечки информации по техническим каналам являются:

При обработке ПДн в ИСПДн возможно возникновение УБПДн за счет реализации следующих технических каналов утечки информации:

Возникновение угроз утечки акустической (речевой) информации, содержащаяся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из-за наличия электромагнитных излучений монитора.

### **3.3. Угрозы несанкционированного доступа.**

Угрозы НСД в ИСПДн с применением программных и программноаппаратных средств реализуются при осуществлении несанкционированного, в 84

том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения), целостности (уничтожения, изменения) и доступности (блокирования) ПДн, и включают в себя:

## **4. Модель угроз безопасности ПДн, обрабатываемых в ИСПДн.**

При обработке ПДн в ИСПДн, возможна реализация следующих видов УБПДн:

### **4.1. Угрозы утечки информации по техническим каналам.**

При обработке ПДн в ИСПДн возможно возникновение УБПДн за счет реализации следующих технических каналов утечки информации:

#### **4.1.1. Угрозы утечки акустической (речевой) информации.**

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, обусловлено наличием функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Утечка акустической (речевой) информации может быть осуществлена:

В ИСПДн не реализованы функции голосового ввода ПДн в ИСПДн. Акустические средства воспроизведения ПДн в ИСПДн не предусмотрены.

Рассмотрение угроз утечки акустической (речевой) информации не целесообразно в связи с отсутствием предпосылок возникновения угроз.

#### **4.1.2. Угрозы утечки видовой информации.**

Угрозы утечки видовой информации реализуются за счет просмотра ПДн с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Утечка видовой информации может быть осуществлена:



В ИСПДн отсутствует возможность неконтролируемого пребывания физических лиц в служебных помещениях или в непосредственной близости от них, соответственно отсутствует возможность непосредственного наблюдения посторонними лицами ПДн.

Рассмотрение угроз утечки видовой информации не целесообразно в связи с отсутствием предпосылок возникновения угроз.

#### **4.1.3. Угрозы утечки информации по каналам ПЭМИН.**

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническими средствами ИСПДн.

Рассмотрение угроз безопасности ПДн, связанных с перехватом ПЭМИН в ИСПДн, избыточно, так как носители ПДн (технические средства ИСПДн, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин) находятся в пределах контролируемой зоны. Утечка ПДн по каналам ПЭМИН - маловероятна из-за несоответствия стоимости средств съема информации и полученной в результате регистрации ПЭМИН информации, а защита ПДн от данного вида угроз - экономически нецелесообразна.

#### **4.2. Угрозы НСД к ПДн, обрабатываемым в ИСПДн.**

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн. Кроме этого, источниками угроз НСД к информации в ИСПДн могут быть аппаратные закладки и отчуждаемые носители вредоносных программ.

В ИСПДн возможны:

#### **5. Общая характеристика источников угроз НСД.**

Источниками угроз НСД в ИСПДн могут быть:

Нарушители:

Внутренние потенциальные нарушители подразделяются на **восемь категорий** в зависимости от способа доступа и полномочий доступа к ПДн (Таблица 4)

**Таблица 4 Категории нарушителей**

<b>Категория нарушителя</b>	<b>Способ доступа и полномочия</b>

Носитель вредоносной программы.

Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо

прикладной программой, то в качестве ее носителя рассматриваются:

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

1. пакеты передаваемых по компьютерной сети сообщений;
2. файлы (текстовые, графические, исполняемые и т.д.).

Аппаратная закладка.

В ИСПДн имеется опасность применения аппаратных средств, предназначенных для регистрации вводимой с клавиатуры информации, например:

В ИСПДн отсутствует возможность неконтролируемого пребывания физических лиц в служебных помещениях или в непосредственной близости от них, соответственно отсутствует возможность установки аппаратных закладок посторонними лицами.

Существование данного источника угроз маловероятно также из-за несоответствия стоимости аппаратных закладок, сложности их скрытой установки и полученной в результате информации.

### **5.1. Общая характеристика уязвимостей ИСПДн.**

**Уязвимость ИСПДн** - недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности персональных данных.

**Причины** возникновения уязвимостей:

К основным группам уязвимостей ИСПДн, относятся:

Характеристика уязвимостей системного ПО.

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем. При этом возможны уязвимости:

Уязвимости в микропрограммах и в средствах операционной системы, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др.

Характеристика уязвимостей прикладного ПО.

К прикладному программному обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

**Прикладные программы общего пользования** - это

**Специальные прикладные программы** - это

Уязвимости прикладного программного обеспечения могут представлять собой:

### **5.3. Характеристика угроз непосредственного доступа в операционную среду ИСПДн.**

Угрозы доступа (проникновения) в операционную среду компьютера и несанкционированного доступа к ПДн связаны с доступом:

Эти угрозы могут быть реализованы в случае получения физического доступа к ИСПДн или, по крайней мере, к средствам ввода информации в ИСПДн:

Угрозы, реализуемые в ходе загрузки операционной системы

Угрозы, реализуемые после загрузки операционной среды независимо от того, какая прикладная программа запускается пользователем

Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ. Большая часть таких угроз - это угрозы внедрения вредоносных программ.

#### 5.4. Общая характеристика УБПДн, реализуемых с использованием протоколов межсетевое взаимодействие.

Классификация угроз, реализуемых по сети, приведена в Таблице 5. В ее основу положено семь первичных признаков классификации.

**Таблица 5 Описание угроз**

№ п/п	Признак классификации	Тип угрозы	Описание

С учетом проведенной классификации можно выделить \_\_\_\_\_ угроз, реализуемых с использованием протоколов межсетевое взаимодействие:

Анализ сетевого трафика.

Сканирование сети.

Угроза выявления пароля.

Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа.

Навязывание ложного маршрута сети.

Внедрение ложного объекта сети.

Отказ в обслуживании.

Удаленный запуск приложений.

#### 5.5. Общая характеристика угроз программно-математических воздействий.

**Программно-математическое воздействие**- это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

Вредоносные программы могут быть внесены (внедрены) как преднамеренно, так и случайно в программное обеспечение, используемое в ИС, в процессе его разработки, сопровождения, модификации и настройки. Кроме этого, вредоносные программы могут быть внесены в процессе эксплуатации ИС с внешних носителей информации или посредством сетевого взаимодействия как в результате НСД, так и случайно пользователями ИС.

Основными видами вредоносных программ являются:

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

#### 5.6. Общая характеристика нетрадиционных информационных каналов.

**Нетрадиционный информационный канал** - это \_\_\_\_\_

Для формирования нетрадиционных каналов могут использоваться методы:

Методы компьютерной стеганографии предназначены для скрытия факта передачи сообщения путем встраивания скрываемой информации во внешне безобидные данные (текстовые, графические, аудио- или видеофайлы) и включают в себя **две группы методов**, основанных:

Нетрадиционные информационные каналы могут быть сформированы на различных уровнях функционирования ИСПДн:

### 5.7. Общая характеристика результатов несанкционированного или случайного доступа.

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

Нарушению конфиденциальности (копирование, неправомерное распространение), которое может быть осуществлено в случае утечки информации за счет:

Нарушению целостности (уничтожение, изменение) за счет воздействия (модификации) на программы и данные пользователя, а также технологическую (системную) информацию, включающую:

Нарушение целостности информации в ИСПДн может также быть вызвано внедрением в нее вредоносной программы программно-аппаратной закладки или воздействием на систему защиты информации или ее элементы.

Кроме этого, в ИСПДн возможно воздействие на технологическую сетевую информацию, которая может обеспечивать функционирование различных средств управления вычислительной сетью:

Нарушению доступности (блокирование) путем формирования (модификации) исходных данных, которые при обработке вызывают неправильное функционирование, отказы аппаратуры или захват (загрузку) вычислительных ресурсов системы, которые необходимы для выполнения программ и работы аппаратуры.

Указанные действия могут привести к нарушению или отказу функционирования практически любых технических средств ИСПДн:

### 8. Определение уровня исходной защищенности ИСПДн

Под уровнем исходной защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (У1).

**Таблица 6 Показатели исходной защищенности ИСПДн**

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению			
2. По наличию соединения с сетями общего пользования:			
3. По встроенным (легальным) операциям с записями баз персональных данных:			
4. По разграничению доступа к персональным данным:			
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
6. По уровню обобщения (обезличивания) персональных данных:			
7. По объему персональных данных, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			

В соответствии с Таблицей Описание угроз, \_\_\_\_\_ % характеристик ИСПДн соответствуют уровню не ниже " \_\_\_\_\_ ", следовательно ИСПДн имеет \_\_\_\_\_ степень исходной защищенности.

**9. Определение вероятности реализации угроз в ИСПДн**

Под вероятностью реализации угрозы поднимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализации конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки.

Вероятность (Y2) определяется по 4 вербальным градациям этого показателя:

**Таблица 7 Вероятность реализации угроз (вербальный показатель)**

<b>Градация</b>	<b>Описание</b>	<b>Вероятность (Y2)</b>

Оценка вероятности реализации угрозы безопасности различными категориями нарушителей приведена в следующей таблице

**Таблица 8 Вероятность реализации угроз (вероятностный показатель)**

<b>Угроза безопасности ПДн</b>	<b>Вероятность реализации угрозы нарушителем категории Кп</b>

По итогам оценки уровня исходной защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы (Таблица 9). Коэффициент реализуемости угрозы рассчитывается по формуле:  $Y = (Y1+Y2)/20$ .

**Таблица 9 Коэффициент реализуемости угрозы**

Угроза безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации угрозы

**1.1. Оценка опасности угроз ИСПДн**

Оценка опасности производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет 3 значения:

**низкая опасность** - .....

**средняя опасность** - .....

**высокая опасность** - .....

Оценка опасности с учетом приведенных критерием представлена в таблице 10.

**Таблица 10 Оценка опасности**

Угроза безопасности ПДн	Опасность угроз

**1.2. Перечень актуальных УБПДн в ИСПДн**

Правила, отнесения угроз к актуальным приведены в Таблице 11.

**Таблица 11 Актуальность угроз**

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	Неактуал ьная	неактуальная	актуальная
Средняя	Неактуал ьная	актуальная	актуальная
Высокая	актуальн ая	актуальная	актуальная
Очень высокая	актуальн ая	актуальная	актуальная

В соответствии с правилами отнесения угроз безопасности к актуальным, для ИСПДн существуют следующие актуальные угрозы.

**Таблица 12 Актуальные угрозы ИСПДн**

<b>Угроза безопасности ПДн</b>	<b>Опасность угроз</b>

Таким образом, актуальными угрозами безопасности ПДн в ИСПДн являются:

**Заключение**

В настоящем документе проведена классификация УБПДн в ИСПДн, дано общее описание УБПДн и построена Модель угроз. В соответствии с требованиями методических документов ФСТЭК России, выявлены актуальные угрозы безопасности ПДн в ИСПДн, на основе которых в дальнейшем должны быть разработаны Требования по обеспечению безопасности ПДн в ИСПДн.

Построенная Модель угроз безопасности ПДн в ИСПДн применима к существующему состоянию ИСПДн при условии соблюдения основных (базовых) исходных данных:

- технические средства ИСПДн находятся в пределах контролируемой зоны;
- ИСПДн физически отделена от сетей общего пользования;
- отсутствует возможность неконтролируемого пребывания посторонних лиц в служебных помещениях ИСПДн и др.

В случае несоблюдения и/или изменения вышеуказанных условий Модель угроз безопасности ПДн в ИСПДн должна быть подвергнута пересмотру.

**Информационные источники:**

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.
2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.
3. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России.
4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

## **ПРАКТИЧЕСКАЯ РАБОТА № 9 ПРАВОВЫЕ ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ**

**Цель:** научиться применять правовые акты в реальных ситуациях при организации защиты информации в учреждениях и на предприятиях, получить опыт разрешения правовых споров в области информационной безопасности, формировать законопослушность.

**Методы и приемы:** анализ, решение задач, проблемное обучение, мозговой штурм, семинар, кейс-метод.

**Ключевые слова:** государственная тайна, коммерческая тайна, персональные данные, защита информации, авторское право, интеллектуальная собственность, охранный документ, программа ЭВМ, база данных.

### **Порядок выполнения работы**

1. Прочитать задачу, найти правовое обоснование и разрешить противоречивую правовую ситуацию.
2. Обсудить найденное решение, обосновать свою позицию аргументами и положениям правовых актов.
3. Решить задачи для самостоятельной работы по индивидуальному заданию

### **Раздел 1: Государственная тайна.**

#### **Задача 1.**

Гражданин Иванов, служил в качестве члена научно-исследовательской группы института "Прогресс".

Иванов дал интервью для журнала «Метрополитен», в котором оценил радиационную обстановку в регионе с целью продемонстрировать суть его технической разработки по определению интенсивности излучения.

Интервью с Ивановым была опубликована и стала общедоступной, и научным руководством Института "Прогресс".

Администрация института подала заявление на Иванова о возбуждении уголовного дела по признакам преступлений, предусмотренных ст. 147 и ст. 183 Уголовного кодекса.

Защитнику Иванова стало известно, что Иванов воспользовался для разработки своего технического устройства сведениями, составляющими коммерческую тайну.

Будет ли Иванов привлечен к уголовной ответственности? Как ему избежать уголовной ответственности?

#### **Задача 2**

Репортер взял интервью у высокопоставленного чиновника Министерства экономического развития. В интервью были указаны сведения о стратегических запасах золота, платины и серебра. В отношении репортера и чиновника было возбуждено уголовное дело за распространение информации, составляющих государственную тайну.

Что нужно предпринять журналисту и чиновнику, чтобы избежать уголовной ответственности по ст. 283 УК РФ?

#### **Задача 3**

Инженер Михайлов, который был гражданином Российской Федерации и инженер Скрипко, который был гражданином Украины, провели совместной научно-исследовательской работу, разработали новую технологию по виртуализации доменов. Оба соавтора имели доступ к сведениям, составляющим государственную тайну. При рассмотрении заявки федеральным органом исполнительной власти по интеллектуальной собственности было установлено, что в новой технологии использованы сведения, составляющие государственную тайну. Какой орган имеет право рассматривать заявки на секретные изобретения, если они относятся к техническим средствам в области разведывательной деятельности?

Может ли в Российской Федерации быть выдан патент на секретное изобретение?

#### **Задача 4**

Химический комбинат г. Дубоссарск осуществил сброс производственных отходов в



реку. Городские власти, получив от санэпидемслужбы города соответствующую информацию, не оповестили граждан об опасности. В результате купающиеся в реке получили ожоги.

Имеется ли вина городской администрации? Приведите правовые нормы, обосновывающие вашу позицию.

#### **Задача 5**

Российский научно-исследовательский институт «Квант» являлся разработчиком и создателем информационной базы данных об испытаниях авиационно-космической техники. Институт получил разрешение Правительства РФ и соответственно своего министерства о направлении соответствующей информации о характеристиках авиационной аппаратуры в аналогичную научную организацию, находящуюся на территории Белоруссии.

Однако представитель ФАПСИ, через которого предполагалось обеспечить передачу этой информации, обратил внимание дирекции института на конфиденциальный характер передаваемых сведений и, ссылаясь на этот факт, отказал НИИ в выделении каналов и средств для передачи информации.

Институт «Квант» обжаловал решение представителя ФАПСИ в Правительство РФ. Оцените ситуацию с точки зрения действующего законодательства [12].

### **Раздел 2: Конфиденциальная информация: персональные данные, служебная тайна, коммерческая тайна**

#### **Задача 6**

Общественная организация «За здоровье нации» обратилась к администрации Аргаяшской птицефабрики с заявлением о предоставлении информации о технике безопасности на предприятии: уровне ПДК в воздухе производственных помещений, уровне травматизма на производстве и выплате компенсаций по здоровьесбережению. Руководство предприятия отказалось удовлетворить просьбу общественной организации, мотивируя свое отказное решение тем, что указанные данные являются конфиденциальной информацией.

Дайте разъяснения по существу сложившейся ситуации, приведите правовые нормы в обоснование своих доводов.

#### **Задача 7**

Сотрудники частной нотариальной конторы «Дело» на одном из своих совещаний приняли решение — создать собственный тайный архив, в котором собирать наиболее интересную частную информацию о всех своих клиентах и по мере необходимости использовать ее в своей повседневной деятельности.

На следующий день был назначен руководитель архива и два эксперта и они начали собирать через своих коллег нужные сведения и данные о клиентах. Однако о факте создания тайного архива в нотариальной конторе «Дело» стало известно одному из клиентов, и он пожаловался на нотариусов в прокуратуру.

Нарушила ли в этом случае контора законодательство? [11]

#### **Задача 8**

Используя электронную сеть «Межсвязь», главный специалист коммерческого банка «Кубыш» Кусочкин в течение двух недель передавал с магнитных носителей информацию в департамент ценных бумаг ЦБ РФ.

При этом он однажды рассказал о содержании направленных в ЦБ сообщений своему другу - юристу Министерства связи Савенко. Савенко, зная, что его товарищи из адвокатской фирмы «Прокруст» готовят иск против «Кубыш», немедленно переправил им полученную информацию. Адвокаты по достоинству оценили полученные сведения, использовали их при подготовке иска и в итоге - выиграли дело у банка. Узнав об этом, председатель правления коммерческого банка «Кубыш» Кубышкин уволил Кусочкина с работы за разглашение коммерческой тайны. Кусочкин не согласился с решением Кубышкина и обжаловал его действия в суде.

Проанализируйте ситуацию с точки зрения норм информационного права и квалифицируйте действия Кусочкина, Савенко и Кубышкина [3].

### **Задача 9**

Журналисты провели расследование совместно с общественной организацией «Маяк» и выявили повышенный уровень радиоизлучения в деревне Дербишево, находящейся на расстоянии 60 км от химкомбината «Маяк». Об этом было рассказано в газете «За правое дело». Имеются ли в действиях журналистов признаки злоупотребления правом?

Оцените эту ситуацию с точки зрения законодательства о средствах массовой информации. Какие меры здесь необходимо принять к нарушителям?

### **Раздел 3: . Интеллектуальная собственность. Авторское право.**

#### **Задача 10**

Лех Я.В. обратился в суд с иском к ООО «Гранада» о взыскании компенсации за нарушение исключительного права на произведение, компенсации морального вреда, возложении обязанности по удалению произведения с сайта.

В обоснование иска указал, что общество разместило на своем сайте литературно-художественный публицистический очерк (документальный рассказ), посвященный дню защиты Земли, автором которого он является Лех. Разрешение на публикацию очерка на сайте ответчика он не давал. Путем размещения на сайте указанного очерка было нарушено его авторское неимущественное право. Представитель ответчика факт размещения произведения истца на сайте не отрицала, исковые требования признала в части компенсации за нарушение ответчиком авторского права истца, при этом ссылаясь на завышенный размер компенсации, заявленный истцом. В части компенсации морального вреда иск не признала, ссылаясь на то, что неимущественные права истца ответчиком не нарушены.

Отмечает, что «незаконно использованный» ответчиком очерк по количеству строк более чем в два раза превышает написанный им рассказ, авторские права на который были приобретены московским продюсером за 1000 долларов. При этом над очерком он работал около 4 месяцев, а рассказ написан за 1 день. Как разрешить этот спор с позиции норм информационного права?

#### **Задача 11**

Смирнов П.Б. обратился в суд с иском к Новиковой Е.О. о защите авторских прав. Свои требования истец мотивирует тем, что на странице интернет-сайта ответчика неправомерно использована фотография, автором которой является истец, без его согласия на воспроизведение и доведение до всеобщего сведения, без заключения с истцом авторского лицензионного договора, без указания и ссылок на источник и автора произведения, что является нарушением ст. 1229, 1265, 1270, 1300 Гражданского кодекса Российской Федерации (далее по тексту ГК РФ). Ответчиком допущено искажение фотографии в частности: кадрирование, обрезка изображения, наложение на фотографию надписи изменение цветового фона изображения. Истец просил взыскать с Новиковой Е.О. денежную компенсацию за нарушение авторских исключительных прав на фотографию (произведение), компенсацию морального вреда за использование фотографии без указания авторства, судебные расходы по обеспечению доказательств нотариусом и расходы по оплате услуг представителя.

Ответчик вину в неправомерном размещении в сети Интернет фотографии не признала, пояснила, что фотографию удалила, ее размещение носило некоммерческий характер. Считает заявленные истцом суммы к взысканию завышенными. Оцените ситуацию с позиции правовых норм. Какое решение должен принять суд?

#### **Задача 12**

Организация «Новые технологии», занимающаяся формированием информационных ресурсов, начала разработку новой программы для государственных информационных систем. Для обеспечения защиты информационных ресурсов в этой системе был использован криптографический алгоритм «КриптТ» компании «Джомолунгма» . Правомерно ли использование этого криптоалгоритма в разрабатываемой программе? Если да, то при каких условиях?

### **Задача 13**

ООО «Холдинг-М» в лице Москвина осуществляло предоставление возмездных Интернет услуг с применением 2-х электронных терминалов «Инфоинтсэйл», на жестких дисках которых установлены и использовались для работы терминала два экземпляра программы для ЭВМ «Microsoft Windows XP Professional», обладателем авторских и смежных прав на которую является «Корпорация Microsoft».

Вышеуказанные экземпляры ЭВМ являются контрафактными по следующим признакам: отсутствуют документы, подтверждающие приобретение копии программы «Microsoft Windows XP Professional»; в корпусе системного блока не имеется сертификата подлинности программы (COA) с наименованием и уникальным буквенно-цифровым ключом программного продукта; отсутствует соглашение с правообладателем об участии в программе корпоративного лицензирования, тем самым ООО «Холдинг-М» использовало с целью получения прибыли программу для ЭВМ «Microsoft Windows XP Professional». Представитель ООО «Холдинг- М» Москвин пояснял, что документов, подтверждающих приобретение обществом операционной «Windows XP» у него не имеется.

Оцените ситуацию с точки зрения авторского права.

**Раздел 4 Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.**

### **Задача 14**

Оператор ПК Абдуллин, согласно своим должностным обязанностям, приеме электронных носителей с материалами обязан был проверять их на наличие вирусов. Пытаясь завершить работу как можно скорее, Абдуллин проигнорировал проверку на антивирусном программном обеспечении.

В результате попадания вируса в компьютерную систему был испорчен готовый к печати оригинал-макет выпуска газеты. Редакция понесла убытки, был нанесен репутационный вред изданию.

Оцените действия Абдуллина с точки зрения действующего законодательства.

### **Задача 15**

Разработчик программного обеспечения Стив несколько лет работал в акционерном обществе "Галатея". В трудовом договоре не было указано на явно имущественные права на созданные программы в процессе трудовой деятельности программиста.

Во время работы Стив разработал эффективную систему автоматизации учета товаров на предприятии. Увидев, что его программа дает значительный экономический эффект, Стив потребовал от руководства доплату к ежемесячному окладу. Руководство рассмотрело вопрос по оплате и отказалось осуществлять доплату, вместо этого они приняли на работу еще одного программиста. Стив, в надежде, что он не сможет прийти к соглашению с компаниями, модифицировал свою программу, в результате чего она перестала функционировать.

Оцените сложившуюся ситуацию с точки зрения действующего законодательства. Как квалифицировать действия Стива?

### **Задача 16**

Программисту Иванову было поручено создать базу данных по финансовым и нематериальным активам предприятия. В целях быстрого выполнения Иванов, стремясь выполнить свою работу как можно быстрее, проигнорировал требования антивирусной защиты. В результате база данных и программная оболочка были повреждены, предприятию пришлось закупать новое программное обеспечение. На программиста было наложено административное взыскание штраф, с чем он не согласился и обжаловал действия администрации.

Имеются ли здесь нарушения законодательства об информации, информатизации, защите информации и трудового права?

**Раздел 5 Неправомерный доступ к информации.**

### **Задача 17**

Адвокат Хорошавин, работая в юридической фирме «Лига А» в качестве помощника

генерального директора, получил несанкционированный доступ к программам других людей и постоянно использовал их. Более того, часть информации, полученной в базах данных, адвокат Хорошавин продал заинтересованным людям. В то же время, из-за несанкционированного проникновения помощника генерального директора в вышеупомянутые программы, в них начали появляться сбои, после чего владельцы источников информации, чтобы найти причину сбоя программного обеспечения провели экспертизу и установили причину сбоев. Владельцы программ и баз данных потребовали строгого наказания Хорошавина. Оцените сложившуюся ситуацию с точки зрения действующего законодательства.

### **Задача 18**

Сельский почтальон по просьбе своей дочери подслушивал телефонные разговоры ее мужа. Он постоянно вскрывал письма и рассказывал об их содержании своей дочери, жалея ее, ведь она могла остаться одна и воспитывать двоих детей, если муж уйдет от нее к другой женщине.

Имеются ли нарушения законодательства?

### **Задачи для самостоятельного решения**

1. Сотрудник завода Чернов попросил у знакомого бухгалтера дистрибутив на установку программы 1С. В процессе развертывания дистрибутива, Черновым была допущена серьезная ошибка и дистрибутив оказался испорченным. Не мудрствуя лукаво, Чернов решил вернуть другой дистрибутив, взятый в коммерческой фирме у другого знакомого бухгалтера. Оцените действия Чернова.
2. Разработчик программного обеспечения Шариков использовал часть алгоритма своего знакомого Кошечкина, уехавшего некоторое время назад в Европу. Шариков зарегистрировал программу в установленном порядке и получил охранный документ. Кошечкин узнал о коммерческом использовании Шариковым программного продукта и подал на него в суд. Необходимо классифицировать действия Шарикова и Кошечкина. Будет ли удовлетворен иск?
3. Петровский получил на телефон сообщение, в котором был прислан одноразовый пароль для входа в личный кабинет банковских транзакций его подруги Ивановской. Однажды Ивановская просила его телефон для проведения транзакций и, по-видимому, «привязала» номер к личному профилю интернет-банка. Петровский помнил номер карты Ивановской и, воспользовавшись одноразовым паролем, перевел часть денежных средств с банковской карты Ивановской на свой расчетный счет. Оцените действия Петровского и Ивановской с точки зрения информационной безопасности и норм права.
4. Гавриков, обладая специальными познаниями в области работы с электронными вычислительными машинами (далее - ЭВМ) и компьютерными программами, используя принадлежащую ему ЭВМ, имеющую подключение к сети Интернет, приобрел путем копирования с сайта «Fishki» компьютерные программы, заведомо предназначенные для несанкционированного копирования компьютерной информации. Впоследствии посредством принадлежащего ему компьютерного оборудования, а также находящихся в его пользовании хостинговых сервисов с доменными именами использовал указанные вредоносные компьютерные программы для заражения 50 ЭВМ пользователей сети Интернет и построения из них контролируемой сети. Построив контролируемую сеть, Гавриков без ведома и согласия пользователей скопировал хранящуюся в памяти зараженных ЭВМ компьютерную информацию, содержащую сведения о логинах и паролях авторизации пользователей на различных Интернет-ресурсах. Данную информацию Гавриков планировал использовать в личных целях. Оцените действия Гаврикова, приведите правовые нормы в обосновании своих доводов.
5. Анисимов работал и занимал различные должности в отделе технической поддержки UNIX Общества с ограниченной ответственностью (далее ООО) «Приват Трейд». С Анисимовым было заключено соглашение о конфиденциальности для работников ООО «Приват Трейд», согласно которого конфиденциальной информацией является техническая,

технологическая, коммерческая (финансовая), организационная или иная используемая в коммерческой деятельности информация, которая обладает действительной или потенциальной коммерческой ценностью в силу ее неизвестности неограниченному кругу третьих лиц, и к которой нет свободного доступа на законном основании.

В период с 2015 по 2016 годы Анисимов, находясь на своем рабочем месте, используя средства авторизации (логин и пароль), предоставленные ООО «Приват Трейд», и имея, в силу исполняемых обязанностей, доступ к информационным носителям, на которых содержится охраняемая компьютерная информация, скопировал на USB - носитель информацию из базы данных ООО «Приват Трейд», а именно: не менее 40.000 записей, содержащих не прошедших проверку имен, фамилий, никнеймов (имена, которые используется при регистрации на интернет сайтах), а так же адресов электронной почты. После чего Анисимов передал вышеуказанную информацию Мусалову, который не был осведомлен о том, что полученная им информация охраняется внутренними документами ООО «Приват Трейд».

Оцените действия Анисимова и Мусалова с правовых позиций действующего законодательства.

6. Закрытое акционерное общество «1С АКЦИОНЕРНОЕ ОБЩЕСТВО» (далее - ЗАО «1С») обратилось в Арбитражный суд Костромской области с иском к обществу с ограниченной ответственностью «Арктур» (далее - ООО «Арктур») о взыскании компенсации за незаконное использование результатов интеллектуальной деятельности в размере 90 000 руб. Исковые требования мотивированы тем, что в ходе обыска сотрудниками ОРЧ БЭП при УВД Костромской области были изъяты два системных блока и ноутбук, при осмотре выявлено, что на жестких дисках установлены компьютерные программы для ведения учета хозяйственной деятельности «1С: Предприятие 7.7. Комплексная поставка (сетевая версия)» и «1С: Предприятие

7.7. ПРОФ Комплексная поставка», имеющие признаки контрафактности. Согласно заключению эксперта от 28.04.2008 на жестких дисках, представленных на экспертизу системных блоков обнаружена информационная база с учетными данными ООО «Арктур», созданная с использованием программы «1С: Предприятие 7.7. Комплексная поставка (сетевая версия)». Запуск предположительно контрафактной программы «1С: Предприятие 7.7. Комплексная поставка (сетевая версия)» без аппаратного HASP-ключа защиты, вопреки штатного режима регламентируемого разработчиком был возможен вследствие модификации исполняемого файла. Оцените исход правового спора, приведите правовые нормы в подтверждение своей позиции.

7. Должностное лицо - индивидуальный предприниматель Сидорова не представила в установленный срок в государственный орган - Управление Федеральной службы государственной регистрации, кадастра и картографии сведения о состоянии использованных в процессе индивидуальной деятельности геодезических пунктов. Имеется ли в действиях Сидоровой правонарушение?

8. В адрес Общества с ограниченной ответственностью «Мираторг», для подтверждения финансово-хозяйственных взаимоотношений выставлено требование об истребовании документов (информации) при проведении мероприятий налогового контроля в отношении Говоровой Н.Н. Конкурсный управляющий Общества с ограниченной ответственностью «Мираторг» (далее также - Общество) Хацевич А.А. сообщил, что требование не получал, несмотря на то, требование в адрес Общества было направлено заказным письмом по юридическому адресу организации и почтовому адресу организации и по адресу конкурсного управляющего. Истребуемые документы (информация) для проведения встречной проверки должны быть представлены в пятидневный срок со дня получения требования. Ходатайства о продлении срока предоставления документов (информации) в соответствии с п.5 ст.93.1 Налогового кодекса Российской Федерации в налоговый орган от обязанного представить соответствующие сведения лица не поступало. Имеется ли в действиях конкурсного управляющего правонарушение? Обоснуйте ответ

правовыми нормами.

9. Заместителем генерального директора ОАО «УТК» по юридической и кадровой работе Громовой было направлено обращение в адрес министра строительства, жилищно-коммунального и дорожного хозяйства Республики Коми и Председателя Государственного Совета Республики Коми, содержащего, в числе прочего, информацию о проводимой работе по подготовке наградных листов для поощрения благодарностью Главы Республики Коми работников ОАО «УТК» - генерального директора Гаврилова и первого заместителя генерального директора - финансового директора Миронова. В соответствии с должностной инструкции Громова обязалась выполнять требования действующего законодательства РФ, приказов, инструкций, положений и иных нормативных актов по обеспечению сохранности конфиденциальной информации, не разглашать и не передавать конфиденциальные сведения, которые будут доверены или станут известны в ходе рабочего процесса во время выполнения должностных обязанностей (договорных) обязанностей. Администрация ОАО «УТК» наложила на Громову административное взыскание за разглашение персональных данных работников, на что Громова не согласилась и обратилась в суд с иском по трудовому спору. Оцените исход правового спора, приведите правовые нормы в подтверждение своей позиции.

10. Руководитель отдела технических разработок ФАПСИ Куликов дал интервью журналу "Горизонты", отметив положительный опыт организации деятельности ФАПСИ в современных условиях. Интервью получило широкий резонанс среди читателей журнала, и редакция журнала выплатила гонорар Куликову. Руководству ФАПСИ стало известно об интервью Куликова и ему был объявлен выговор за выступление без разрешения руководства. Куликов расценил данное наказание как нарушение ч.1 ст. 29 Конституции РФ. Как можно расценить спор с точки зрения действующего законодательства?

11. Программист Якупов и адвокат Гришин создали компьютерную программу, для экспертной оценки подлинности рукописных текстов. Якупов и Гришин подали заявку в патентное ведомство России на выдачу патента на полезную модель. Патентное ведомство отклонило их заявку, указав, что программы для компьютеров не признаются патентоспособными изобретениями. Разработчики не согласились с данным отказом и обратились в суд. Необходимо дать разрешение данной спорной ситуации.

12. На совещании юридических и физических лиц, работающих в области информатики и телекоммуникаций, заместитель руководителя Торгово-промышленной палаты Российской Федерации Кошель в резкой форме покритиковал те организации, которые копируют и используют программные и технические средства информатики без разрешения собственника и допускают иные нарушения этических норм. А буквально на следующий день это выступление Кошеля было без сокращений опубликовано в «Вестях» и обиженные организации потребовали от руководителя Торгово-промышленной палаты снятия с должности выступавшего за нарушение норм Национального кодекса деятельности в области информатики и телекоммуникаций. Необходимо определить, как должен быть разрешен этот спор.

13. На пленарном заседании торгово-промышленной палаты, посвященном взаимодействию в области развития сферы телекоммуникаций в регионе, вице-президент палаты Голенищев подверг резкой критике руководителей тех организаций, которые только «имитируют деятельность». Большой фрагмент стенограммы встречи был опубликован в областной газете. Обиженные руководители телекоммуникационных предприятий потребовали публикации опровержения в газете, а также снятия с должности вице-президента Голенищева за нарушение им норм «Положения об этике», принятом в Торгово-промышленной палате в качестве локального акта внутреннего распорядка. Вам нужно определить, как нужно решить спор.

14. Программист Войнович и его приятель техник-связист Саламатов обратились в Министерство связи с просьбой выделить им интернет-коммуникации для консалтинговой деятельности зарубежным партнерам. В удовлетворении заявления им было отказано. Войнович и Саламатов обратились за защитой прав предпринимателей в прокуратуру.

Необходимо определить нарушен ли в этом случае порядок выделения ведомственных сетей связи юридическим и физическим лицам и как должен поступить прокурор города.

15. Гражданка Никанорова заподозрила своего мужа в измене и, установила специальную программу ему на телефон, пока он спал. Также она приобрела диктофонное устройство с дистанционным управлением, выполненное в виде дизайнерской зажигалки. Проанализировав детализацию звонков, полученную с помощью установленного программного обеспечения и диктофонные записи, гражданка Никанорова убедилась в правоте своих подозрений относительно неверности супруга, после чего подала на развод.

Супруг гражданки Никаноровой написал заявление о преступлении, совершенной его женой. Признаки какого преступного деяния были описаны в заявлении супруга? Укажите правовые нормы.

16. Писательница Левит получила большой гонорар за изданные в Китае ее книги по личностному развитию. Гонорар был перечислен на ее индивидуальный расчетный счет в «Уралоптбанк». Левит планировала использовать большую часть этих денежных средств на содержание приюта для животных «Спаси меня» известного зоозащитника Даллакяна, поэтому не подала налоговую декларацию о доходах. Налоговая инспекция запросила сведения о доходах Левит в «Уралоптбанк», банк сначала ответил отказом, а потом все-таки предоставил эти сведения, на основании которых налоговый инспектор выставил Левит предписание в виде штрафа и пени за неуплаченный налог на доходы. Разгневанная писательница подала на суд и налоговую инспекцию в суд. Как вы думаете, какое решение примет суд? Обоснуйте правовыми нормами свою позицию.

17. Заядлый охотник Михайлов купил на рынке бинокль повышенной видимости для использования его на охоте. Его приятель Дремов увидев такой бинокль, попросил его на некоторое время у Михайлова с целью подглядывания за своей женой, которая в соседнем квартале работала няней у состоятельных бизнесменов. Оцените действия Михайлова и Дремова с точки зрения действующего законодательства.

18. Начальником управления образования городского округа города Котельнича Червяковой в адрес руководителей образовательных учреждений направлено письмо с требованием о предоставлении в управление образования городского округа города Котельнича сведений об оплате ими и их подчиненными транспортного, земельного налога, налога на имущество. Указанные сведения представлены руководителями образовательных учреждений в управление образования городского округа города Котельнича и в последующем были переданы начальником управления образования городского округа города Котельнича Червяковой в администрацию города Котельнича. Должностными обязанностями Червяковой не предусмотрено осуществление сбора, хранения, использования и распространения персональных данных руководителей и работников образовательных учреждений г. Котельнича, не связанных с осуществлением ими трудовой деятельности в образовательных учреждениях. Оцените ситуацию с точки зрения действующего законодательства.

19. Сотрудник рекрутингового агентства Жорин проводил отбор претендентов на должность личного помощника руководителя крупного промышленного предприятия. За хорошее выполнение этой работы ему была обещана персональная выплата от руководителя. Требования к будущему личному помощнику были следующие: высшее образование, модельная внешность, разговорный английский, кроме того девушка не должна быть замужем. Желая получить обещанную выплату Жорин в свободное от работы время съездил по адресам потенциальных претенденток и узнал от соседей их семейный статус. Как вы думаете имеет ли место нарушение законодательства?

#### **Информационные источники:**

1. <http://www.garant.ru>
2. <http://www.consultHnt.ru>
3. <https://rospravosudie.com>

## **ПРИМЕНЕНИЕ ИНВЕРСИОННОГО МЕТОДА ДЛЯ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ.**

**Цель:** ознакомиться с инверсионным анализом ТРИЗ (теории решения изобретательских задач), научиться использовать инверсионный анализ для решения задач информационной безопасности, мотивировать обучающихся к расширению методологических оснований для будущей профессиональной деятельности.

**Методы и приемы:** работа по алгоритму, анализ, синтез, инвертирование, мозговой штурм, самостоятельная работа, решение задач.

### **Порядок выполнения работы**

1. Изучить теоретические сведения, при необходимости обратиться к интернет-источникам
2. Изучить учебную задачу
3. Применить инверсионный метод для самостоятельного решения задач информационной безопасности.

### **Краткие теоретические сведения.**

Инверсионный метод (Диверсионный анализ) — это один из разделов ТРИЗ (теории решения изобретательских задач - основоположник Альтшуллер Г.С.), направленный на выявление и предотвращение вредных явлений в системах различного генезиса — технических, информационных, организационных [1].

Суть метода состоит в инвертировании проблемной ситуации при выявлении технических противоречий в системе, то есть в создании системной диверсии.

Метод позволяет выявить явные и скрытые причины возможных отказов, уязвимостей, рисков, иных вредных явлений в системе, тем самым появляется возможность спрогнозировать и предотвратить проявление проблем такого рода, предусмотрев соответствующие меры при разработке или модификации системы. Таким образом, метод применяется:

- для поиска причин вредных явлений;
- для прогнозирования возможных вредных явлений.

Применительно к информационной системе, реализованной посредством информационно-коммуникационных технологий, задача состоит в ее «взломе» и несанкционированном доступе к информации.

Как правило, инверсионный метод реализуется через последовательные стадии:

1. Инвертирование задачи.
2. Формулирование «диверсионных гипотез».
3. Выявление «диверсионных ресурсов».
4. Тестирование «диверсионных гипотез».

В более сложных ситуациях может быть использован более широкий набор инструментов анализа [3].

Рассмотрим алгоритм решения учебной задачи с применением инверсионного метода и возможные схемы решений.

**Учебная задача «Об электронной оболочке»:** Необходимо определить перечень уязвимостей электронной оболочки личных профилей профессорско-преподавательского состава (далее - ППС) вуза, предложить меры по устранению потенциальных угроз.

Согласно ГОСТ Р 56545-2015 «уязвимость» - это недостаток (слабость) программного (программно-технического) средства или ИС в целом, который (которая) может быть использована для реализации угроз безопасности информации.

Информационная система - это совокупность содержащейся в базах данных (далее по тексту - БД) информации и обеспечивающих ее обработку информационных технологий и технических средств.



### **Стадия 1:** Инвертирование задачи.

Переформулируем задачу в виде: «Как взломать электронную оболочку личных профилей ППС и получить доступ к конфиденциальной информации?»

### **Стадия 2:** Формулирование диверсионных гипотез.

В вузе принят негласный шаблон составления логина профиля из фамилии и инициалов имени и отчества преподавателя. Таким образом, логин можно составить, исходя из сведений о фамилии, имени и отчества, данные сведения являются открытыми и доступны на сайте университета.

После определения логина, остается подобрать пароль.

Несложно просто подсмотреть пароль, либо при выполнении каких-либо работ попросить интересующего нас преподавателя войти в его профиль, ссылаясь на неработающий свой или какие-то неполадки системы. Этот способ допустим, если «добытчик» пароля является сотрудником и в силу своего должностного положения может осуществить описанную последовательность действий.

Если такая мера неосуществима, пароль можно вычислить, пользуясь специальным программным обеспечением. При известном логине, вычислительных ресурсов только «взлома» пароля требуется немного.

Существует множество программ, две наиболее популярные - advnced arcbIye Password Recovery и Visaul Zip Password Recovery Processor.

Кроме вышеперечисленных способов

можно попытаться подобрать пароль с клавиатуры, используя известную информацию о человеке - день рождения, имя любимого питомца, и т.д.

Таким образом, предложены три диверсионные гипотезы для решения данной задачи.

### **Стадия 3:** выявление диверсионных ресурсов.

На этой стадии необходимо составить список ресурсов, которые способствуют реализации диверсионных гипотез.

Перечень диверсионных ресурсов может быть таким:

- наличие шаблона составления логина;
- низкий уровень дисциплины ППС в области информационной безопасности;
- незнание и/или несоблюдение элементарных правил сохранения своих идентификаторов и аутентификаторов;
- малая обеспеченность компьютерной техникой рабочих мест ППС, когда за одним персональным компьютером закреплено несколько сотрудников.

**Стадия 4:** тестирование диверсионных гипотез - определение процедуры тестирования и проведение тестов.

Процедура тестирования состоит в экспериментальной проверке «взлома» электронной оболочки личных профилей ППС, то есть реализации выдвинутых гипотез на стадии 2.

Проверкой установлено, что логины были определены по шаблону «фамилия+инициалы». Среднее время определения логинов - 10 минут.

Подбор паролей с помощью программного обеспечения к трем профилям осуществлен в среднем в течение 30 минут, таким образом, тестирование подтвердило правоту диверсионных гипотез и наличие уязвимостей в описанной информационной системе.

При подведении итогов решения учебной задачи были предложены следующие способы усиления информационной защиты электронной оболочки:

- рекомендация замены логина и пароля пользователя после первого входа и активации профиля;
- разработка инструкции для сотрудников о необходимости сохранения аутентификаторов и идентификаторов;
- регулярный инструктаж сотрудников по соблюдению правил обеспечения информационной безопасности системы.

### **Задачи для самостоятельного решения.**

a. **Задача «О защите интеллектуальной собственности свободными лицензиями».** Определить уязвимости для нарушения авторского права при распространении интеллектуальных продуктов в правовом поле свободных лицензий. Для определенности рассмотреть семейства Common Public License, Creative Commons Zero, Creative Commons Attribution, GNU General Public License.

b. **Задача «О применении нейросетей для выявления террористических угроз».** В США потратили миллиарды долларов на разработку искусственного интеллекта, способного заменить человеческие ресурсы (проект ELINT- electronic intelligence) в разведке путем прослушивания и анализа разговоров по телефонам и анализа контента информационных ресурсов, используемых потенциальными террористами.

Когда проект ELINT был готов, президент Джимми Картер отозвал всех американских агентов с Ближнего Востока. С тех пор Соединенные Штаты не задержали ни одного крупного террориста. С помощью инверсионного анализа определите причину неудач.

c. **Задача «О проведении банковских транзакций».** Платежи физических лиц в настоящее время все чаще производятся с помощью смартфонов через личный профиль интернет-банка. Подтверждение платежей физическим лицом происходит через одноразовые пароли, высылаемые на привязанный номер мобильного оператора смс-сообщением. Определить уязвимости данной системы, используя методы инверсионного анализа.

d. **Задача «Защиты персональных данных».** С помощью инверсионного анализа определить уязвимости автоматизированной информационной системы (АИС) обработки персональных данных учреждения профессионального образования. Исходные данные АИС определить самостоятельно, используя сайт образовательного учреждения.

e. **Задача «О системе «Платон».** Используя инверсионный анализ, определите уязвимости системы «Платон» взимания платы с большегрузных автомобилей. Предложите меры для эффективного функционирования данной системы.

f. **Задача «Сетевой город».** В настоящее время в общеобразовательных школах введена система «Сетевой город». Определить уязвимости и способы защиты данной учебной системы.

g. **Задача «О стратегической космической онлайн игре EVE Online».** Взлом профиля противника в названной командной он-лайн игре дает множество игровых преимуществ, от перераспределения ресурсов, в том числе и реальных денежных средств, до тактического преимущества на отдельном этапе этой массовой многопользовательской онлайн игры. Определите уязвимости профиля, используя инверсионный анализ и знание особенностей семиуровневой модели OSI.

h. **Задача «О сопровождении в социальной сети ВКонтакте».** Исследователи неоднократно поднимали вопрос о потенциальной угрозе национальной безопасности России, реализованной в социальных сетях. Экстремистские группы социальных сетей представляют реальную угрозу национальной безопасности страны, вовлекая до миллиона молодых граждан России, пропагандируя идеи политического экстремизма, национального и гендерного превосходства и неравенства. Подобных групп в социальных сетях немало и, если какие-то из них блокируются техническими службами по заявлениям равнодушных пользователей, то на их месте появляется множество других с таким же опасным контентом. Используя инверсионный анализ, предложите меры по защите подрастающего поколения от негативного информационного воздействия экстремистских групп на примере социальной сети «ВКонтакте».

### **Информационные источники:**

1. Абрамов О.Ю. Диверсионный анализ Технических Систем на переходном этапе развития - [Электронный ресурс] // URL: <http://triz-summit.ru/file.php/id/f5015/nme/TRIZ-> (дата обращения: 15.02.2017)

2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.
3. Буслов Д.И., Холкин И.Н. Как, используя диверсионный анализ ТРИЗ, найти критическую уязвимость, грозящую безопасности SP Hn // Математика и информационные технологии в нефтегазовом комплексе. 2015. №2. URL: <http://cyberlenink.ru/article/n/kk-ispolzuy-diversionnyu-nliz-triz-nyti-kriticheskuyu-uyzvimost-grozyschuyu-bezopsnosti-sp-hn> (дата обращения: 11.04.2017).
4. Вишнепольски С. Как выявлять причины вреда и устранять риски. Инверсионный метод риск-анализа. iBooks Edition. Mx EPublishing, 2013. 131 с.

## **ПРИЛОЖЕНИЕ 2 ТЕСТЫ ДЛЯ САМОПРОВЕРКИ.**

### **ТЕСТ 1**

1. **К каким мерам защиты относится политика безопасности?**
  - а) к административным;
  - б) к законодательным;
  - в) к программно-техническим;
  - г) к процедурным.
2. **В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу?**
  - а) CL;
  - б) списки полномочий субъектов;
  - в) атрибутные схемы.
3. **Как называется свойство информации, означающее отсутствие неправомерных, и не предусмотренных ее владельцем изменений?**
  - а) целостность;
  - б) апеллируемость;
  - в) доступность;
  - г) конфиденциальность;
  - д) аутентичность.
4. **К основным принципам построения системы защиты АИС относятся:**
  - а) открытость;
  - б) взаимозаменяемость подсистем защиты;
  - в) минимизация привилегий;
  - г) комплексность;
5. **Диспетчер доступа...**
  - а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа;
  - б) ... использует атрибутные схемы для представления матрицы доступа;
  - в) ... выступает посредником при всех обращениях субъектов к объектам;
  - г) ... фиксирует информацию о попытках доступа в системном журнале;
6. **Какие предположения включает неформальная модель нарушителя?**
  - а) о возможностях нарушителя;
  - б) о категориях лиц, к которым может принадлежать нарушитель;
  - в) о привычках нарушителя;
  - г) о предыдущих атаках, осуществленных нарушителем;
  - д) об уровне знаний нарушителя.
7. **Что представляет собой доктрина информационной безопасности РФ?**
  - а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности;
  - б) федеральный закон, регулирующий правоотношения в области информационной

безопасности;

в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов;

г) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

**8. К какому виду мер защиты информации относится утвержденная программа работ в области безопасности?**

- а) политика безопасности верхнего уровня;
- б) политика безопасности среднего уровня;
- в) политика безопасности нижнего уровня;
- г) принцип минимизации привилегий;
- д) защита поддерживающей инфраструктуры.

**9. Чтобы подписать сообщение электронной цифровой подписью, используются:**

- а) открытый ключ отправителя;
- б) открытый ключ получателя;
- в) закрытый ключ отправителя;
- г) закрытый ключ получателя.

**10. Какова последовательность подписания сообщений с помощью ЭЦП?**

- а) вычисляется хэш, затем хэш зашифровывается;
- б) сообщение зашифровывается, после чего результат хэшируется;
- в) при подписании сообщение зашифровывается, при проверке вычисляется хэш;
- г) вычисляется хэш исходного сообщения, после чего оно зашифровывается.

**11. В чем заключается такое свойство функции хэширования  $H$  как стойкость к коллизиям первого рода?**

а) Для любого хэша  $h$  должно быть практически невозможно вычислить или подобрать такое  $x$ , что  $H(x) = h$ .

б) Должно быть практически невозможно вычислить или подобрать любую пару различных сообщений  $x$  и  $y$  для которых  $H(x) = H(y)$ ;

в) Длина хэша должна быть фиксированной независимо от длины входного сообщения;

Ключ к тесту: 1а, 2б, 3а, 4б, 5в, 6б, 7б, 8а, 9в, 10в, 11а.

## ТЕСТ 2

**1. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это**

- 1. информационная война
- 2. информационное оружие
- 3. информационное превосходство

**2. Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.**

- 1. служебная информация
- 2. коммерческая тайна
- 3. банковская тайна
- 4. конфиденциальная информация

**3. Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена**

- 1. конфиденциальность
- 2. целостность
- 3. доступность
- 4. аутентичность
- 5. апеллируемость

4. **Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано**
  1. надежность
  2. точность
  3. контролируемость
  4. устойчивость
  5. доступность
5. **Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования, которое спасает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.**
  1. принцип системности
  2. принцип комплексности
  3. принцип непрерывной защиты
  4. принцип разумной достаточности
  5. принцип гибкости системы
6. **В классификацию вирусов по способу заражения входят**
  1. опасные
  2. файловые
  3. резидентные
  4. загрузочные
  5. файлово -загрузочные
  6. нерезидентные
7. **Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это...**
  1. комплексное обеспечение И Б
  2. безопасность АС
  3. угроза И Б
  4. атака на АС
  5. политика безопасности
8. **Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются:**
  1. компаньон - вирусами
  2. черви
  3. паразитические
  4. студенческие
  5. призраки
  6. стеле-вирусы
9. **К видам системы обнаружения атак относятся :**
  1. системы, обнаружения атаки на ОС
  2. системы, обнаружения атаки на конкретные приложения
  3. системы, обнаружения атаки на удаленных БД
  4. все варианты верны
10. **Автоматизированная система должна обеспечивать**
  1. надежность
  2. доступность
  3. целостность
  4. контролируемость
11. **Основными компонентами парольной системы являются**
  1. интерфейс администратора
  2. хранимая копия пароля

3. база данных учетных записей
4. все варианты верны

**12. Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это**

1. идентификатор пользователя
2. пароль пользователя
3. учетная запись пользователя
4. парольная система

**13. К принципам информационной безопасности относятся**

1. скрытость
2. масштабность
3. системность
4. законность
5. открытости алгоритмов

**14. К вирусам, изменяющим среду обитания относятся:**

1. черви
2. студенческие
3. полиморфные
4. спутники

**15. Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это...**

1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Безопасность данных

**16. Система физической безопасности включает в себя следующие подсистемы:**

1. оценка обстановки
2. скрытность
3. строительные препятствия
4. аварийная и пожарная сигнализация

**17. Какие степени сложности устройства Вам известны**

1. упрощенные
2. простые
3. сложные
4. оптические
5. встроенные

**18. К механическим системам защиты относятся:**

1. проволока
2. стена
3. сигнализация

**19. Какие компоненты входят в комплекс защиты охраняемых объектов:**

1. датчики
2. телевизионная система
3. лес

**20. К выполняемой функции защиты относится:**

1. внешняя защита
2. внутренняя защита
3. все варианты верны

**21. Набор аппаратных и программных средств для обеспечения сохранности,**

**доступности и конфиденциальности данных:**

1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Безопасность данных

**22. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспреещения доступа к ним это:**

1. информационная война
2. информационное оружие
3. информационное превосходство

**23. Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:**

1. государственная тайна
2. коммерческая тайна
3. банковская тайна
4. конфиденциальная информация

**24. Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:**

1. конфиденциальность
2. целостность
3. доступность
4. аутентичность
5. апеллируемость

**25. Гарантия точного и полного выполнения команд в АС:**

1. надежность
2. точность
3. контролируемость
4. устойчивость
5. доступность

**26. Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми:**

1. принцип системности
2. принцип комплексности
3. принцип непрерывности
4. принцип разумной достаточности
5. принцип гибкости системы

**27. Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности:**

1. Комплексное обеспечение информационной безопасности
2. Безопасность АС
3. Угроза информационной безопасности
4. атака на автоматизированную систему
5. политика безопасности

**28. Особенности информационного оружия являются:**

1. системность
2. открытость
3. универсальность
4. скрытность

**29. К функциям информационной безопасности относятся:**

1. выявление источников внутренних и внешних угроз
2. страхование информационных ресурсов
3. защита государственных информационных ресурсов
4. подготовка специалистов по обеспечению информационной безопасности
5. все ответы верны

**30. К типам угроз безопасности парольных систем относятся**

1. словарная атака
2. тотальный перебор
3. атака на основе психологии
4. разглашение параметров учетной записи
5. все варианты ответа верны

**31. К вирусам не изменяющим среду обитания относятся:**

1. черви
2. студенческие
3. полиморфные
4. спутники

**32. Хранение паролей может осуществляться**

1. в виде сверток
2. в открытом виде
3. в закрытом виде
4. в зашифрованном виде
5. все варианты ответа верны

**33. Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется:**

1. ревизором
2. иммунизатором
3. сканером
4. доктора и фаги.

**34. Указать недостатки, имеющиеся у антивирусной программы ревизор:**

1. неспособность поймать вирус в момент его появления в системе
2. небольшая скорость поиска вирусов
3. невозможность определить вирус в новых файлах ( в электронной почте, на дискете)
4. все варианты верны

**35. В соответствии с особенностями алгоритма вирусы можно разделить на два класса:**

1. Вирусы, изменяющие среду обитания, но не распространяющиеся
2. Вирусы, изменяющие среду обитания при распространении
3. Вирусы, не изменяющие среду обитания при распространении
4. Вирусы, не изменяющие среду обитания и не способные к распространению в дальнейшем

**36. К достоинствам технических средств защиты относятся:**

1. регулярный контроль
2. создание комплексных систем защиты
3. степень сложности устройства
4. Все варианты верны

**37. К тщательно контролируемым зонам относятся:**

1. рабочее место администратора
2. архив
3. рабочее место пользователя
4. все варианты верны



**38. К системам оповещения относятся:**

1. инфракрасные датчики
2. электрические датчики
3. электромеханические датчики
4. электрохимические датчики

**39. К оборонительным системам защиты относятся:**

1. проволочные ограждения
2. звуковые установки
3. датчики
4. покрышки

**40. К национальным интересам РФ в информационной сфере относятся:**

1. Реализация конституционных прав на доступ к информации
  2. Защита информации, обеспечивающей личную безопасность
  3. Защита независимости, суверенитета, государственной и территориальной целостности
  4. Политическая экономическая и социальная стабильность
  5. Сохранение и оздоровлении окружающей среды
- Ключ к тесту: 1-1, 2-4, 3-1, 4-1, 5-5, 6-3,6, 7-1, 8-2, 9-4, 10-2,3, 11-1,3, 12, 13-3,4,5 14-3,15-1, 16-1,3,4, 17-2,3, 18-1,2,4, 19-1,2, 20-3,21-2, 22-2, 23-2, 24-2, 25-2,26-4, 27-5, 28-3,4, 29-5, 30-5, 31-1, 32-1,2,4 33-3, 34-4, 35-2,3, 36-2, 37-4, 38-1,2, 39-1,2, 40-1.

**ПРИЛОЖЕНИЕ 3**  
**СОДЕРЖАНИЕ КОНЦЕПЦИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ**  
**БЕЗОПАСНОСТИ УЧРЕЖДЕНИЯ**

- Общие положения
- Описание объекта защиты
  - о Назначение и основные функции информационной системы
  - о Группы задач, решаемых в информационной системе
  - о Классификация пользователей системы
  - о Организационная структура обслуживающего персонала
  - о Структура и состав комплекса программно-технических средств
  - о Корпоративная сеть предприятия

---

- Серверы
- Рабочие станции
- Линии связи и активное сетевое оборудование
- Виды информационных ресурсов, хранимых и обрабатываемых в системе
- Структура информационных потоков
- Внутренние информационные потоки
  - Внешние информационные потоки
- Характеристика каналов взаимодействия с другими системами и точек входа
- Основные факторы, влияющие на информационную безопасность предприятия
- Основные принципы обеспечения информационной безопасности
- Организация работ по защите информации
- Меры обеспечения информационной безопасности
  - о Меры \_\_\_\_\_ обеспечения \_\_\_\_\_ информационной \_\_\_\_\_ безопасности организационного уровня
  - о Меры обеспечения информационной безопасности процедурного уровня
- Распределение ответственности и порядок взаимодействия
- Порядок категорирования защищаемой информации
- Модель нарушителя информационной безопасности

---

- о Внутренние нарушители

- o Внешние нарушители
- Модель угроз информационной безопасности
  - o Защита информационных компонентов и группы угроз
  - o Угрозы, реализуемые с использованием технических средств
  - o Угрозы, реализуемые с использованием программных средств
  - o Угрозы утечки информации по техническим каналам связи
- Требования по обеспечению информационной безопасности

---

  - o Требования к составу основных подсистем СОИБ
  - o Требования к подсистеме управления политикой безопасности
  - o Требования к подсистеме анализа и управления рисками
  - o Требования к подсистеме идентификации и аутентификации
  - o Требования к подсистеме разграничения доступа
  - o Требования к подсистеме протоколирования и пассивного аудита
  - o Требования к подсистеме активного аудита безопасности
  - o Требования к подсистеме контроля целостности
  - o Требования к подсистеме контроля защищенности
  - o Требования к подсистеме «удостоверяющий центр»
  - o Требования к подсистеме сегментирования и межсетевого экранирования
  - o Требования к подсистеме VPN
  - o Требования к подсистеме антивирусной защиты
  - o Требования к подсистеме фильтрации контента
  - o Требования к подсистеме управления безопасностью
  - o Требования к подсистеме предотвращения утечки информации по техническим каналам
- Технические требования к смежным подсистемам
  - o Требования к структурированной кабельной системе
  - o Требования по физической защите
- Ответственность сотрудников за нарушение безопасности
- Механизм реализации концепции

**Информационный источник:**

<http://securitypolicy.ru> - (Дата обращения: 08.04.2017).

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

### Стандарты

ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.

ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические условия. Госстандарт России. - М., 1995.

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. - М., 2006.

ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие требования. Госстандарт России. - М., 2006.

ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем». - М.: Стандартинформ, 2015.

### Используемая литература

5. Абрамов О.Ю. Диверсионный анализ Технических Систем на переходном этапе развития - [Электронный ресурс] // URL: <http://triz-summit.ru/file.php/id/f5015/nme/TRIZ-> (дата обращения: 15.02.2017)
6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.
7. Буслов Д.И., Холкин И.Н. Как, используя диверсионный анализ ТРИЗ, найти критическую уязвимость, грозящую безопасности SP Hn // Математика и информационные технологии в нефтегазовом комплексе. 2015. №2. URL: <http://cyberlenink.ru/article/n/kk-ispolzuy-diversionnyu-nliz-triz-nyti-kriticheskuyu-uyzvimost-grozyschuyu-bezopsnosti-sp-hn> (дата обращения: 11.04.2017).
8. Вишнепольски С. Как выявлять причины вреда и устранять риски. Инверсионный метод риск-анализа. iBooks Edition. Мх EPublishing, 2013. 131 с.
9. Галатенко В.А. Идентификация и аутентификация, управление доступом [Электронный ресурс]: <http://citforum.ru/security/articles/galatenko/> (дата обращения - 01.03.2017)
10. Гафарова Е.А., Азарова Е.А., Гафаров В.Ф., Гафаров М.Ф. Применение инверсионного метода для выявления уязвимостей информационной системы в обучении магистрантов. // Информационные технологии в экономике, образовании и бизнеса. Саратов: Издательство «ЦПМ Бизнес», 2017, с.22-28, ISBN 978-59909175-3-8
11. Гафарова Е.А., Гафаров М.Ф. О необходимости педагогического сопровождения в социальной сети «ВКонтакте» // Личность, семья и общество: вопросы педагогики и психологии: сб. ст. по матер. LXVII междунар. науч.-практ. конф. № 8(65). - Новосибирск: СибАК, 2016. - С. 19-23.
12. Гафарова Е.А. О возможности использования открытых лицензий для защиты интеллектуальных прав создателей научных и образовательных ресурсов // Сб. материалов II-ой международной научно-практической конференции. 2016 Издательство: Научноиздательский центр "Империум" (Москва), с.46-49
13. Гафарова Е.А. К вопросу обеспечения информационно психологической безопасности подрастающего поколения в условиях

интенсификации воздействия интернет-источников.// Научная дискуссия: инновации в современном мире: сб. ст. по материалам LVI Международной научно-практической конференции «Научная дискуссия: инновации в современном мире». - № 12(55). - М., Изд. «Интернаука», 2016. - С. 115-118.

14. Гафарова Е.А., Сеницын Ф.В. К вопросу проектирования онтологий предметной области при подготовке магистров по направлению информационная безопасность.// Инновационные технологии в подготовке современных профессиональных кадров: Опыт, проблемы. Сборник научных трудов. 2016, Челябинский филиал РАНХиГС, 56-59 с.

15. Грицай Л.А. Информационная война в социальных сетях как угроза национальной безопасности России // Современные научные исследования и инновации. 2014. № 10 - [Электронный ресурс] - URL: <http://web.snuk.ru/issues/2014/10/38607> (Дата обращения: 24.05.2016).

16. Кармановский Н.С., Михайличенко О.В., Савков С.В. Организационно-правовое и методическое обеспечение информационной безопасности: Учебное пособие. - СПб.: НИУ ИТМО, 2013. - 148 с.

17. Коноваленко С. А., Королев И. Д. Выявление уязвимостей информационных систем. // Инновации в науке: сб. ст. по матер. LXI междунар. науч.-практ. конф. № 9(58). - Новосибирск: СибАК, 2016. - С. 12-20.

18. Мезенов А.С., Гафарова Е.А. О реализации конституционного права граждан на доступ к информации в условиях интенсификации сетевого взаимодействия.//Сборник научных трудов конференции «Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы», 2016, Издательство: Челябинский филиал РАНХиГС, с.94-99

19. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.

20. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России.

21. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / А. А. Стрельцов [и др.]; под ред. А. А. Стрельцова. — М.: Издательский центр «Академия», 2008. — 256 с. ISBN 978-5-7695-4240-4

22. Приказ Министерства образования и науки РФ от 1 декабря 2016 г. № 1513 “Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры)”- [Электронный ресурс] // URL: <http://www.grnt.ru/products/ipo/prime/doc/71471182/#ixzz4WszFeZNC> - (дата обращения 15.02.2017)

23. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

24. Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении доктрины информационной безопасности Российской Федерации” [Электронный ресурс] /- URL: <http://www.grnt.ru/hotlw/federl/1036728/> - (Дата обращения: 08.04.2017).

25. Фомичева Т.Г. Лабораторный практикум по курсу «Компьютерные технологии и в правовой практике» Южно-Российский государственный технический университет, УДК 004.9:34 (076.5) ББК 67.0 Ф 76Новочеркасск 2008

26. Чубукова С.Г. Организационное и правовое обеспечение информационной

безопасности. Учебник и практикум. ISBN: 9785991676076 Год издания: 2016. Серия: Профессиональное образование. Издательство: Юрайт.

27. Шиллер В.В., Шелудков Н.Н. Российские социальные сети как потенциальная угроза национальной безопасности России (на примере сайтов «Одноклассики» и «ВКонтакте») // Вестник КемГУ. 2013. № 3 (55). URL: <http://cyberlenink.ru/article/n/rossiyskie-sotsilnye-seti-kk-potentsi...> (Дата обращения: 21.07.2016).

28. Kpln S., Visnepolschi S., Zlotin B., Zusmn . New tools for failure & risk nlysis.n Introduction to nticipatory Filure Determinton (FD) nd The Theory of Scenrio Structuring. Idetion Interntionl Inc., 1999.

#### **Электронные ресурсы.**

[Электронный ресурс] // URL: <https://www.anti-malware.ru/node/13626#part4>- (Дата обращения: 22.02.2017)

[Электронный ресурс] // URL: <http://www.e-nigm.ru/articles/>- (Дата обращения: 22.02.2017)

[Электронный ресурс] // URL: <http://www.iso27000.ru/zkonodtelstvo/normtivnye-dokumenty-fstek-rossii>- (Дата обращения: 22.02.2017)

[Электронный ресурс] // URL: <http://www.intuit.ru> - (Дата обращения: 22.02.2017)

[Электронный ресурс] // URL: <http://www.garant.ru/>- (Дата обращения: 22.02.2017)

[Электронный ресурс] // URL: <http://www.n.n.n.n>.- (Дата обращения: 22.02.2017)

[Электронный ресурс] // URL: <https://rospravosudie.com>- (Дата обращения: 22.02.2017)

[Электронный ресурс] // URL: <https://www.scienceforum.ru>- (Дата обращения: 22.02.2017)

[Электронный ресурс] // URL: <http://securitypolicy.ru> - (Дата обращения: 08.04.2017).

[Электронный ресурс] // URL: <http://fstec.ru/>- (Дата обращения: 22.02.2017)

[Электронный ресурс] // URL: <https://ru.wikipedia.org> - (Дата обращения: 22.02.2017)

Приложение 3  
к рабочей программе дисциплины ОП.05 Основы алгоритмизации и  
программирования

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«Национальный исследовательский ядерный университет «МИФИ»

**Димитровградский инженерно-технологический институт –**  
филиал федерального государственного автономного образовательного учреждения высшего  
образования «Национальный исследовательский ядерный университет «МИФИ»  
(ДИТИ НИЯУ МИФИ)



УТВЕРЖДАЮ

Директор техникума ДИТИ НИЯУ МИФИ

Н.А. Домнина

15 апреля 2021 г.

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ**  
**по применению активных и интерактивных методов обучения**  
**при изучении учебной дисциплины (МДК, модуля)**  
**ОП.01 Основы информационной безопасности**  
(наименование учебной дисциплины)

программы подготовки специалистов среднего звена по специальности  
**10.02.05 Обеспечение информационной безопасности автоматизированных**  
**СИСТЕМ**

Код, наименование специальности

Форма обучения очная

Учебный цикл ОП

Составитель: Н.А. Шульга, преподаватель техникума ДИТИ НИЯУ МИФИ

Димитровград 2021

## Оглавление

<b><u>ЦЕЛИ ПРИМЕНЕНИЯ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ В ПРЕПОДАВАНИИ УЧЕБНОЙ ДИСЦИПЛИНЫ</u></b>	6
<b><u>ПЕДАГОГИЧЕСКАЯ ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ ИННОВАЦИИ В ПРЕПОДАВАНИИ УЧЕБНОЙ ДИСЦИПЛИНЫ</u></b>	6
<b><u>КРАТКАЯ ХАРАКТЕРИСТИКА ИННОВАЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ</u></b>	ОШИБ
<b><u>Интерактивные технологии обучения</u></b>	Ошибк
<b><u>Компьютерные технологии</u></b>	8
<b><u>Возможности технологии компьютерного обучения</u></b>	11
<b><u>ЗАКЛЮЧЕНИЕ</u></b>	ОШИБ
<b><u>БИБЛИОГРАФИЧЕСКИЙ СПИСОК, ВКЛЮЧАЯ ИНТЕРНЕТ-РЕСУРСЫ</u></b>	15
<b><u>ПРИЛОЖЕНИЕ 1</u></b>	16
<b><u>Описание урока с применением презентации</u></b>	16
<b><u>Пример презентации «Тест самоконтроля»</u></b>	17

## **Цели применения инновационных технологий в преподавании учебной дисциплины**

Целью инновационного подхода к учебному процессу, является развитие у учащихся возможностей осваивать новый опыт на основе целенаправленного формирования творческого и критического мышления, опыта и инструментария исследователя.

Главной целью инновационных технологий образования является подготовка человека к жизни в постоянно меняющемся мире. Сущность такого обучения состоит в ориентации учебного процесса на потенциальные возможности человека и их реализацию. Образование должно развивать механизмы инновационной деятельности, находить творческие способы решения жизненно важных проблем, способствовать превращению творчества в норму и форму существования человека.

Задачей технологии как науки является выявление совокупности закономерностей с целью определения и использования на практике наиболее эффективных, последовательных образовательных действий, требующих меньших затрат времени.

И поэтому педагоги внедряют в практику такие инновационные технологии как:

- технологии дифференциации и индивидуализации;
- проектные технологии, предполагающие, организацию урока в форме самостоятельного проектирования учебного материала, который в дальнейшем структурируется и моделируется в определенной форме: графической, знаковой или символической;
- технологии проблемного обучения;
- интерактивные технологии;
- информационные технологии:
- мультимедиа – уроки, которые проводятся на основе компьютерных обучающих программ;
- уроки на основе электронных учебников;
- презентации.

## **Педагогическая эффективность использования инновации в преподавании учебной дисциплины**

Всплеск интереса к этой теме использования информационных технологий в преподавании в методической литературе и создание комплектов наглядных пособий пришлось на вторую половину XX века. С течением времени образовательные учреждения утратили старые пособия и сегодня не имеют возможности приобрести новые, ввиду их отсутствия старые методические разработки по наглядности уже потеряли свою актуальность.

Несмотря на трудности, информационные технологии уже широко применяются преподавателями, у которых сложилось своё мнение о положительных и отрицательных сторонах их применения. Этот опыт привлёк внимание представителей педагогической науки. Появилось большое количество исследовательских работ по теме применения информационных технологий. Положительными сторонами применения ИТО можно считать:

1. Использование ИТО помогает обеспечить тесное взаимодействие между преподавателем и обучаемым даже в условиях дистанционного образования. ИТО предоставляют самые широкие возможности. Описание творческого процесса, его результаты могут быть представлены и обсуждены на электронной конференции, опубликованы в электронном издании, размещены на Web-сайте учебного заведения.



Например, на смену рукописным тематическим журналам (исторические, литературные и др.) не только в вузах, но и во многих школах, гимназиях, лицеях появляются электронные журналы, для которых нет проблем с тиражированием и распространением. Каждый желающий может ознакомиться с их материалами через Internet, а при отсутствии у учебного заведения своего Web-сайта - через локальную сеть.



2. ИТО расширяют возможности образовательной среды как разнообразными программными средствами, так и методами развития креативности обучаемых. К числу таких программных средств относятся моделирующие программы, поисковые, интеллектуальные обучающие, экспертные системы, программы для проведения деловых игр. Фактически во всех современных электронных учебниках делается акцент на развитие творческого мышления. С этой целью в них предлагаются задания эвристического, творческого характера, ставятся вопросы, на которые невозможно дать однозначный ответ, и т.д. Коммуникационные технологии позволяют по-новому реализовывать методы, активизирующие творческую активность. Обучаемые могут включиться в дискуссии, которые проводятся не только в аудитории или классе, но и виртуально, например на сайтах периодических изданий, учебных центров. В выполнении совместных творческих проектов могут участвовать учащиеся различных учебных заведений.

3. Новое содержание образовательной среды создает и дополнительные возможности для стимулирования любознательности обучаемого. Одним из таких стимулов является возможность удовлетворить свое любопытство, благодаря широчайшим возможностям глобальной сети Internet предоставляется доступ к электронным библиотекам (научно-техническим, научно-методическим, справочным и т.д.), интерактивным базам данных культурных, научных и информационных центров, энциклопедиям, словарям. Через Internet обучаемый может обратиться с вопросом по заинтересовавшей его проблеме не только к своему наставнику, но и к ведущим отечественным и зарубежным специалистам, вынести его на обсуждение в электронной конференции или чате. Само разнообразие информации, предлагающейся в образовательной среде, интегрированной в мировое информационное пространство, помогает педагогу подвести обучаемых к поиску собственного взгляда на суть изучаемой проблемы. Развитию любознательности обучаемых, привитию интереса к поисково-исследовательской деятельности помогает также возможность работы в виртуальных научных лабораториях, проведение компьютерных экспериментов с помощью моделирующих программ.

4. Создаваемые на сайтах учебных заведений персональные web-страницы педагогов предоставляют дополнительные возможности и для того, чтобы открыть обучаемым "дверь" в свою творческую мастерскую. На таких страницах можно показать не только учебные материалы, но и свои научные публикации, проспекты проводимых исследований, лучшие работы "учеников, превзошедших учителя". Выход в мировое информационное пространство позволяет увидеть множество образцов креативности: на сайтах, рассказывающих о деятельности научно-исследовательских центров и отдельных научно-исследовательских институтов; в материалах электронных научных журналов и конференций; результатах конкурсов творческих проектов и дистанционных олимпиад; на персональных web-страницах учащихся, студентов, преподавателей, ученых всего мира.

Персональный компьютер можно использовать как универсальное техническое средство обучения (ТСО). Такое ТСО позволяет упорядоченно хранить огромное количество материала и готовых разработок уроков.

Систематическое использование персонального компьютера на уроках приводит к целому ряду любопытных последствий:

-  Повышение уровня использования наглядности на уроке.
-  Повышение производительности труда.

- ✚ Установление межпредметных связей.
- ✚ Появляется возможность организации проектной деятельности учащихся по созданию учебных программ под руководством учителей.
- ✚ Преподаватель, создающий, или использующий информационные технологии, вынужден обращать огромное внимание подачи учебного материала. Что положительным образом сказывается на уровне знаний учащихся.
- ✚ Изменяется к лучшему взаимоотношения с учениками далекими от литературы, особенно с увлеченными компьютерами. Они начинают видеть в учителе "родственную душу".
- ✚ Изменяется отношение к компьютеру, как к дорогой, увлекательной игрушке. Студенты начинают воспринимать его в качестве универсального инструмента для работы в любой области человеческой деятельности.

Использование новых информационных технологий способно существенно углубить содержание материала, а применение нетрадиционных методик обучения может оказать заметное влияние на формирование практических умений и навыков учащихся в освоении материала.

Вместе с тем существует достаточное количество проблем связанных с внедрением ИТО в образовательный процесс и их негативное влияние на успехи учеников, психологическое и физическое здоровье школьников. Среди них:

- ✚ Сложность восприятия больших объемов информации с экрана дисплея;
- ✚ Отсутствие непосредственного и регулярного контроля над ходом выполнения учебного плана;
- ✚ Нарушение взаимодействия преподаватель-ученик, так как компьютер не может заменить полностью преподавателя. Только преподаватель имеет возможность заинтересовать учащихся, побудить в них любознательность, завоевать их доверие, направить их на те, или иные аспекты изучаемого предмета, вознаградить за усилия и заставить учиться.

Не смотря на эти проблемы нельзя не отметить, что информационные технологии:

- ✚ Формируют высокую степень мотивации, повышают интерес к процессу обучения;
- ✚ Повышают интенсивность обучения;
- ✚ Позволяют достигнуть индивидуализации обучения;
- ✚ Обеспечивают объективность оценивания результатов;
- ✚ Увеличивают долю самостоятельной работы.

### Компьютерные технологии

Компьютерные технологии обучения — это процессы сбора, переработки, хранения и передачи информации обучаемому посредством компьютера. К настоящему времени наибольшее распространение получили такие технологические направления, в которых компьютер является:

- ✚ средством для предоставления учебного материала учащимся с целью передачи знаний;
- ✚ средством информационной поддержки учебных процессов как дополнительный источник информации;
- ✚ средством для определения уровня знаний и контроля за усвоением учебного материала;
- ✚ универсальным тренажёром для приобретения навыков практического применения знаний;
- ✚ средством для проведения учебных экспериментов и деловых игр по

предмету изучения;

✚ одним из важнейших элементов в будущей профессиональной деятельности обучаемого.

На современном этапе во многих профессиональных учебных заведениях разрабатываются и используются как отдельные программные продукты учебного назначения, так и автоматизированные обучающие системы (АОС) по различным учебным дисциплинам. АОС включает в себя комплекс учебно-методических материалов (демонстрационных, теоретических, практических, контролирующих), компьютерные программы, которые управляют процессом обучения.



Рисунок1. Возможности мультимедиа технологий

С появлением операционной системы Windows в сфере профессионального обучения открылись новые возможности. Прежде всего, это доступность диалогового общения в так называемых интерактивных программах. Кроме того, стало осуществимым широкое использование графики (рисунков, схем, диаграмм, чертежей, карт, фотографий). Применение графических иллюстраций в учебных компьютерных системах позволяет на новом уровне передавать информацию обучаемому и улучшить ее понимание.

Возросшая производительность персональных компьютеров сделала возможным достаточно широкое применение технологий мультимедиа. Современное профессиональное обучение уже трудно представить без этих технологий, которые позволяют расширить области применения компьютеров в учебном процессе.

Новые возможности в системе профессионального образования открывает гипертекстовая технология. Гипертекст (от англ. hypertext — "сверхтекст"), или гипертекстовая система, — это совокупность разнообразной информации, которая может располагаться не только в разных файлах, но и на разных компьютерах. Основная черта гипертекста — это возможность переходов по так называемым гиперссылкам, которые представлены либо в виде специально сформированного текста, либо определённого графического изображения. Одновременно на экране компьютера может быть несколько гиперссылок, и каждая из них определяет свой маршрут "путешествия".

Современную гипертекстовую обучающую систему отличает удобная среда обучения, в которой легко находить нужную информацию, возвращаться к уже пройденному материалу и т. п.

Автоматизированные обучающие системы, построенные на основе гипертекстовой технологии, обеспечивают лучшую обучаемость не только благодаря наглядности представляемой информации. Использование динамического, т. е. изменяющегося, гипертекста позволяет провести диагностику обучаемого, а затем автоматически выбрать один из возможных уровней изучения одной и той же темы. Гипертекстовые обучающие системы представляют информацию так, что и сам обучаемый, следуя графическим или текстовым ссылкам, может использовать различные схемы работы с материалом.

Применение компьютерных технологий в системе профессионального образования способствует реализации следующих педагогических целей:

- ✚ развитие личности обучаемого, подготовка к самостоятельной продуктивной профессиональной деятельности;
- ✚ реализация социального заказа, обусловленного потребностями современного общества;
- ✚ интенсификация образовательного процесса в профессиональной школе.

Инновационные технологии обучения, отражающие суть будущей профессии, формируют профессиональные качества специалиста, являются своеобразным полигоном, на котором учащиеся могут отработать профессиональные навыки в условиях, приближенных к реальным.

Обучающая, воспитывающая, развивающая функция урока обеспечивается различными средствами. Одним из таких средств является компьютер. Но, чтобы применение компьютера на предметных уроках давало положительные результаты, необходима правильная организация работы учебного процесса:

1. Урок должен проводить преподаватель, т.к. он обучен методике преподавания.
2. Компьютерные задания должны быть составлены в соответствии с содержанием учебного предмета и методикой его преподавания, развивающие, активизирующие мыслительную деятельность и формирующие учебную деятельность учащихся.
3. Учащиеся должны уметь обращаться с компьютером на уровне, необходимом для выполнения компьютерных заданий.
4. Учащиеся должны заниматься в специальном кабинете, оборудованном в соответствии с установленными гигиеническими.

**При разработке компьютерной поддержки предмета необходимо определить:**

1. Какие темы стоит “поддерживать” компьютерными заданиями и для решения каких дидактических задач.
2. Какие программные средства целесообразно использовать для создания и выполнения компьютерных заданий.
3. Какие предварительные умения работы на компьютере должны быть сформированы у детей.
4. Какие уроки целесообразно делать компьютерными.
5. Как организовать компьютерные занятия.



Рис.2 Приоритетные принципы и подходы образования

### **Возможности технологии компьютерного обучения**

Функциональные свойства современных компьютерных и коммуникационных технологий предоставляют образовательному процессу реализацию следующих возможностей:

- ✚ неограниченные возможности сбора, хранения, передачи, преобразования, анализа и применения разнообразной по своей природе информации;
- ✚ повышение доступности образования, с расширением форм получения образования;
- ✚ обеспечение непрерывности получения образования и повышения квалификации в течение всего активного периода жизни;
- ✚ развитие личностно-ориентированного обучения, дополнительного и опережающего образования;
- ✚ значительное расширение и совершенствование организационного обеспечения образовательного процесса (виртуальные школы, лаборатории, университеты, другое);
- ✚ повышение активности субъектов в организации образовательного процесса;
- ✚ создание единой информационно-образовательной среды обучения и не только одного региона, но страны и мирового сообщества в целом;
- ✚ независимость образовательного процесса от места и времени обучения;
- ✚ значительное совершенствование методического и программного обеспечения образовательного процесса;
- ✚ обеспечение возможности выбора индивидуальной траектории обучения;
- ✚ развитие самостоятельной творчески развитой личности;
- ✚ развитие самостоятельной поисковой деятельности обучающегося;
- ✚ повышение мотивационной стороны обучения.

Все перечисленные возможности компьютерной техники позволяют разрабатывать новые технологии обучения, которые могут способствовать повышению качества образования.

В зарубежной практике принято следующее понимание технологий обучения на основе активного использования компьютера и информационных технологий.

CAI	Computer Aided Instruction	Компьютерное программированное обучение
CAL	Computer Aided Learning	Изучение с помощью компьютера
CBL	Computer Based Learning	Изучение на базе компьютера
CBT	Computer Based Training	Обучение на базе компьютера
CAA	Computer Aided Assessment	Оценивание с помощью компьютера

В определенном смысле подобная классификация является весьма условной, поскольку в ней, по сути дела, происходит пересечение отдельных технологий.

В этом можно убедиться, рассмотрев более детально каждую из них.

*Компьютерное программированное обучение (CAI)* — это технология, обеспечивающая реализацию механизма программированного обучения с помощью соответствующих компьютерных программ.

*Изучение с помощью компьютера (CAL)* предполагает самостоятельную работу обучаемого по изучению нового материала с помощью различных средств, в том числе и компьютера. Характер учебной деятельности здесь не регламентируется, изучение может осуществляться и при поддержке наборов *инструкций*, что и составляет суть метода программированного обучения, лежащего в основе технологии CAI.

*Изучение на базе компьютера (CBL)* отличает от предыдущей технологии то, что если там возможно использование самых разнообразных средств обучения (в том числе и традиционных — учебников, аудио- и видеозаписей и т.п.), то в этой технологии предполагается использование преимущественно программных средств, обеспечивающих эффективную самостоятельную работу обучающихся.

*Обучение на базе компьютера (CBT)* подразумевает всевозможные формы передачи знаний обучаемому (с участием педагога и без) и, по существу, пересекается с вышеназванными.

*Оценивание с помощью компьютера (CAA)* может представлять собой и самостоятельную технологию контроля, однако на практике компьютерный контроль входит составным элементом в другие технологии обучения.

В нашем представлении такой подход к классификации технологий компьютерного обучения и контроля не совсем корректен, **ПОСКОЛЬКУ** практически невозможно разделить представленные технологии на совершенно самостоятельные и, скорее всего, такое разделение нецелесообразно.

Существуют *педагогические цели разработки технологии компьютерного обучения и использования компьютерных средств*.

1) развитие личности обучаемого, подготовка индивида к комфортной жизни в условиях информационного общества:

- развитие мышления, (например, наглядно-действенного, наглядно-образного, интуитивного, творческого, теоретического видов мышления);
- эстетическое воспитание (например, за счет использования возможностей компьютерной графики, технологии мультимедиа);
- развитие коммуникативных способностей;
- формирование умений принимать правильное решение или предлагать варианты решения в сложной ситуации (например, за счет использования компьютерных обучающих игр, ориентированных на оптимизацию деятельности по принятию решения);

- развитие умений осуществлять экспериментально-исследовательскую деятельность (например, за счет реализации возможностей компьютерного моделирования или использования оборудования, сопрягаемого с ЭВМ);

- формирование информационной культуры, умений осуществлять обработку информации (например, за счет использования интегрированных пользовательских пакетов, различных графических и музыкальных редакторов);

2) интенсификация всех уровней учебно-воспитательного процесса:

- повышение эффективности и качества процесса обучения за счет реализации возможностей компьютерных средств обучения;

- обеспечение побудительных мотивов (стимулов), обуславливающих активизацию познавательной деятельности обучающихся (например, за счет компьютерной визуализации учебной информации, вкрапления игровых ситуаций, возможности управления, выбора режима учебной деятельности);

- углубление межпредметных связей за счет использования современных средств обработки информации, в том числе и аудиовизуальной, при решении задач различных предметных областей.

3) совершенствование информационно-методического обеспечения педагогической деятельности:

- значительное расширение информационно-методической поддержки педагогов и обучающихся;

- расширение возможностей общения и сотрудничества на основе компьютерных средств коммуникации;

- предоставление возможностей непрерывного повышения квалификации и переподготовки независимо от возраста, географии проживания и времени;

- создание единой информационно-образовательной среды на основе активного использования компьютерных сетей различного уровня (глобальных, корпоративных, локальных).

Разработка и внедрение технологий компьютерного обучения может значительно повлиять на весь образовательный процесс в компьютерных средах обучения. Положительные результаты при внедрении компьютерных технологий обучения дает организация занятий на основе рационального сочетания индивидуальных, групповых (малых групп) и коллективных форм обучения; видоизменение характера общения между преподавателями и обучающимися, использование личностно-деятельностной модели и личностно-ориентированного подхода в обучении. Компьютерные технологии обучения и контроля становятся основой инновационных образовательных технологий, поскольку позволяют реализовать индивидуальные запросы обучающегося, обеспечивают развитие личности и повышают уровень доступности получения образования и непрерывного повышения квалификации.

Не отрицая важности классификации ИТО, заметим, что для их эффективного применения педагогу в первую очередь необходимо ориентироваться в соответствующем программном обеспечении.

Разработка полноценных программных продуктов учебного назначения - дорогостоящее дело, поскольку для этого необходима совместная работа высококвалифицированных специалистов: психологов, преподавателей-предметников, компьютерных дизайнеров, программистов. Многие крупные зарубежные фирмы и ряд отечественных производителей программной продукции финансируют проекты создания компьютерных учебных систем в учебных заведениях и ведут собственные разработки в этой области.

Программное обеспечение, использующееся в ИТО, можно разбить на несколько категорий:

- ✚ обучающие, контролирующие и тренировочные системы,
- ✚ системы для поиска информации,
- ✚ моделирующие программы,
- ✚ микромиры,
- ✚ инструментальные средства познавательного характера,
- ✚ инструментальные средства универсального характера,
- ✚ инструментальные средства для обеспечения коммуникаций.

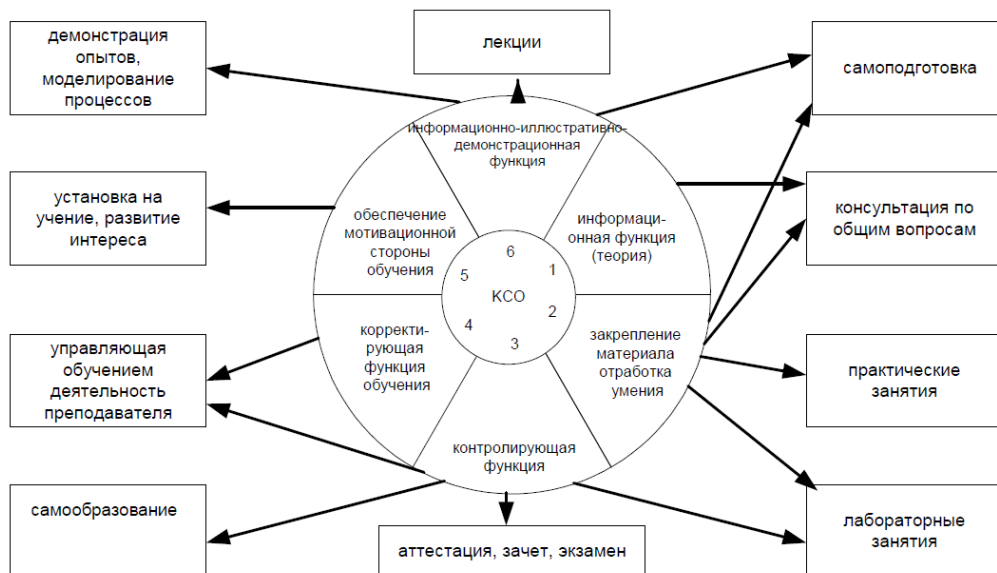


Рисунок 3. Функции и формы применения компьютерных средств обучения

Под инструментальными средствами понимаются программы, обеспечивающие возможность создания новых электронных ресурсов: файлов различного формата, баз данных, программных модулей, отдельных программ и программных комплексов. Такие средства могут быть предметно-ориентированными, а могут и практически не зависеть от специфики конкретных задач и областей применения.



Рисунок 4. Программное обеспечение образовательного процесса

Специфика новых информационных технологий заключается в том, что они представляют пользователям - преподавателям и учащимся - громадные возможности. Использование компьютеров усиливает интерес к предмету. Позволяет учителю сэкономить массу времени, которое он раньше затрачивал на меловые записи и рисунки на доске. Для работы заранее подготавливаются файлы на дискете, содержащие план



изучаемой темы, необходимые даты, термины, схемы, вопросы. Изображение проецируется на экраны мониторов.

**Библиографический список, включая Интернет-ресурсы**

1. Боголюбов В.И. Инновационные технологии в педагогике. /В.И. Боголюбов // Школьные технологии. - 2021. - №1.
2. Дахин А.Н. Образовательные технологии: сущность, классификация, эффективность/ А.Н. Дахин // Школьные технологии. - 2018 - №2.
3. Захарова И.Г. Информационные технологии в образовании/ И.Г. Захарова. - М.: Академия, 2019.
4. Интернет в гуманитарном образовании/ [Под ред. Полат Е. С.]. - М.: Владос, 2018. - 272с. - 169с.
5. Андреев В.И. Педагогика: Учебный курс для творческого саморазвития / В.И. Андреев. – Казань, 2019 – С. 440-441.

### Описание урока с применением презентации

1. **Тема занятия:** Программные средства создания и обработки анимации. Обзор средств создания и обработки Gif-анимации.

2. **Тип занятия:** лекция

3. **Цели занятия:** *-цель познания:* изучить виды анимации и программы для их создания.

*-цель развития(формируемые компетенции):* ОК03, ОК 06, ОК 09, ОК 10, ПК 2.4, В 14, В 15, В16

*-цель воспитания:* осознать для себя пользу в приобретении знаний и умений по организации работы с программой, способствовать формированию интереса к дисциплине.

4. **Задачи урока:** узнать о основных характеристиках анимации, научиться различать виды анимации и программы для их создания, закрепить старые и приобрести новые знания об основных понятиях компьютерной анимации.

#### 5. Краткое описание хода урока

№ п/п	Элементы учебного занятия	Содержание и методы обучения	Приб. время, мин.	Используемые средства обучения
1.	Организационное начало занятия.	1. Приветствие. 2. Проверка явки и готовности к занятию. 3. Сообщение темы и постановка целей занятия.	5	Учебный журнал
2.	Актуализация опорных знаний	Беседа: • Давайте вспомним с какими программами мы работали? Перечислите классы этих программ? • С помощью каких программ мы создавали компьютерную графику? • Какие виды компьютерной графики мы изучили?	10	
3.	Мотивация деятельности.  Основная часть	Рано или поздно у каждого человека возникает желание творить. Некоторые рисуют на стенах, другие сочиняют стихи или музыку. Но есть и такие, которые создают на компьютере свои собственные виртуальные миры, живущие по их собственным законам. Тому, как это делается, и посвящен наш сегодняшний обзор. Все пакеты 2D и 3D-моделирования и анимации, рассмотренные здесь, не требуют никакого специального оборудования и при желании купить эти программы не составит никакого труда. Лекция: • 3D анимация 3DS MAX; Maya ; Rhinoceros ; TrueSpace • 2D анимация Moho; Animation Stand; Mirage ; Animo 6.0 • GIF-формат Easy GIF Animator Pro; Ulead GIF Animator; Microsoft GIF Animator; CoffeeCup GIF Animator • Интерфейс Ulead GIF Animator	45	Мультимедийный проектор, экран, ПК, презентация №1
4.	Рефлексия.	На этой лекции новым было.....Мне были известны вопросы.....Мы изучали вопрос.....Я осознал.....Я уяснил.....Я испытал затруднения...Мне понравилось...Я понял, что это можно применить для...	10	
5.	Закрепление изученного материала.	Тест Самоконтроля	15	Презентация №2
6.	Подведение итогов занятия	Выставление оценок работающим на уроках студентам	2	Учебный журнал
7.	Организация	Исследовать конспект.	3	тетрадь

самост. внеауд. работы студентов	Продумать сюжет своего проекта.		
----------------------------------	---------------------------------	--	--

**6. Знания, умения, навыки и качества, которые актуализируют/приобретут/закрепят/др. ученики в ходе урока:** *Узнают о основных характеристиках анимации, научатся различать виды анимации и программы для их создания, закрепят старые и приобретут новые знания об основных понятиях компьютерной анимации.*

**Пример презентации «Тест самоконтроля»  
(Презентация №2 представленного проекта)**

<p align="center"><b>Тест самоконтроля</b></p> <p align="center"><b>«Gif - Анимация»</b></p> <p align="center"><small>Мой университет – www.moi-mu.ru</small></p>	<table border="1"> <thead> <tr> <th>Ив</th> <th>Вопрос</th> <th>Пв</th> </tr> </thead> <tbody> <tr> <td></td> <td align="center"><b>1</b></td> <td></td> </tr> <tr> <td><b>Что является основной характеристикой анимации?</b></td> <td> <ol style="list-style-type: none"> <li>Плавность движения</li> <li>Число кадров</li> <li>Красота эффектов</li> <li>Прорисовка персонажа</li> </ol> </td> <td> <b>Graphics Interchange Format – это:</b> <ol style="list-style-type: none"> <li>Gif89</li> <li>Gif92</li> <li>Gif98</li> <li>Gif87</li> </ol> </td> </tr> </tbody> </table> <p align="center"><small>Мой университет – www.moi-mu.ru</small></p>	Ив	Вопрос	Пв		<b>1</b>		<b>Что является основной характеристикой анимации?</b>	<ol style="list-style-type: none"> <li>Плавность движения</li> <li>Число кадров</li> <li>Красота эффектов</li> <li>Прорисовка персонажа</li> </ol>	<b>Graphics Interchange Format – это:</b> <ol style="list-style-type: none"> <li>Gif89</li> <li>Gif92</li> <li>Gif98</li> <li>Gif87</li> </ol>									
Ив	Вопрос	Пв																	
	<b>1</b>																		
<b>Что является основной характеристикой анимации?</b>	<ol style="list-style-type: none"> <li>Плавность движения</li> <li>Число кадров</li> <li>Красота эффектов</li> <li>Прорисовка персонажа</li> </ol>	<b>Graphics Interchange Format – это:</b> <ol style="list-style-type: none"> <li>Gif89</li> <li>Gif92</li> <li>Gif98</li> <li>Gif87</li> </ol>																	
<table border="1"> <thead> <tr> <th>Ив</th> <th>Вопрос</th> <th>Пв</th> </tr> </thead> <tbody> <tr> <td></td> <td align="center"><b>2</b></td> <td></td> </tr> <tr> <td><b>Палитра формата Gif поддерживает :</b></td> <td> <ol style="list-style-type: none"> <li>512 цветов</li> <li>256 цветов</li> <li>16 цветов</li> <li>1024 цвета</li> </ol> </td> <td> <b>Какой метод сжатия применяется в графическом формате gif?</b> <ol style="list-style-type: none"> <li>PK3</li> <li>Rar</li> <li>Lzw</li> <li>Zip</li> </ol> </td> </tr> </tbody> </table> <p align="center"><small>Мой университет – www.moi-mu.ru</small></p>	Ив	Вопрос	Пв		<b>2</b>		<b>Палитра формата Gif поддерживает :</b>	<ol style="list-style-type: none"> <li>512 цветов</li> <li>256 цветов</li> <li>16 цветов</li> <li>1024 цвета</li> </ol>	<b>Какой метод сжатия применяется в графическом формате gif?</b> <ol style="list-style-type: none"> <li>PK3</li> <li>Rar</li> <li>Lzw</li> <li>Zip</li> </ol>	<table border="1"> <thead> <tr> <th>Ив</th> <th>Вопрос</th> <th>Пв</th> </tr> </thead> <tbody> <tr> <td></td> <td align="center"><b>3</b></td> <td></td> </tr> <tr> <td><b>Максимальный размер картинки формата Gif в пикселях – это:</b></td> <td> <ol style="list-style-type: none"> <li>256x256</li> <li>2048x2048</li> <li>500x500</li> <li>65535x65535</li> </ol> </td> <td> <b>Время показа одного кадра находится в пределе от (сек.) :</b> <ol style="list-style-type: none"> <li>1 до 100</li> <li>1/100 до 655</li> <li>1/256 до 512</li> <li>1/100 до 256</li> </ol> </td> </tr> </tbody> </table> <p align="center"><small>Мой университет – www.moi-mu.ru</small></p>	Ив	Вопрос	Пв		<b>3</b>		<b>Максимальный размер картинки формата Gif в пикселях – это:</b>	<ol style="list-style-type: none"> <li>256x256</li> <li>2048x2048</li> <li>500x500</li> <li>65535x65535</li> </ol>	<b>Время показа одного кадра находится в пределе от (сек.) :</b> <ol style="list-style-type: none"> <li>1 до 100</li> <li>1/100 до 655</li> <li>1/256 до 512</li> <li>1/100 до 256</li> </ol>
Ив	Вопрос	Пв																	
	<b>2</b>																		
<b>Палитра формата Gif поддерживает :</b>	<ol style="list-style-type: none"> <li>512 цветов</li> <li>256 цветов</li> <li>16 цветов</li> <li>1024 цвета</li> </ol>	<b>Какой метод сжатия применяется в графическом формате gif?</b> <ol style="list-style-type: none"> <li>PK3</li> <li>Rar</li> <li>Lzw</li> <li>Zip</li> </ol>																	
Ив	Вопрос	Пв																	
	<b>3</b>																		
<b>Максимальный размер картинки формата Gif в пикселях – это:</b>	<ol style="list-style-type: none"> <li>256x256</li> <li>2048x2048</li> <li>500x500</li> <li>65535x65535</li> </ol>	<b>Время показа одного кадра находится в пределе от (сек.) :</b> <ol style="list-style-type: none"> <li>1 до 100</li> <li>1/100 до 655</li> <li>1/256 до 512</li> <li>1/100 до 256</li> </ol>																	
<table border="1"> <thead> <tr> <th>Ив</th> <th>Вопрос</th> <th>Пв</th> </tr> </thead> <tbody> <tr> <td></td> <td align="center"><b>4</b></td> <td></td> </tr> <tr> <td><b>Уменьшится или увеличится размер gif файла после сжатия его в zip архив</b></td> <td> <ol style="list-style-type: none"> <li>Вёретка газет</li> <li>Создание звуковых эффектов</li> <li>Создание анимации, баннеров</li> <li>Создание аватарки, фильма</li> </ol> </td> <td> <b>Назначение Ulead Gif Animator - ...</b> <ol style="list-style-type: none"> <li>Увеличится</li> <li>Не изменится</li> <li>Уменьшится</li> <li>Нельзя сжать</li> </ol> </td> </tr> </tbody> </table> <p align="center"><small>Мой университет – www.moi-mu.ru</small></p>	Ив	Вопрос	Пв		<b>4</b>		<b>Уменьшится или увеличится размер gif файла после сжатия его в zip архив</b>	<ol style="list-style-type: none"> <li>Вёретка газет</li> <li>Создание звуковых эффектов</li> <li>Создание анимации, баннеров</li> <li>Создание аватарки, фильма</li> </ol>	<b>Назначение Ulead Gif Animator - ...</b> <ol style="list-style-type: none"> <li>Увеличится</li> <li>Не изменится</li> <li>Уменьшится</li> <li>Нельзя сжать</li> </ol>	<table border="1"> <thead> <tr> <th>Ив</th> <th>Вопрос</th> <th>Пв</th> </tr> </thead> <tbody> <tr> <td></td> <td align="center"><b>5</b></td> <td></td> </tr> <tr> <td><b>Программы, позволяющие создавать анимацию:</b></td> <td> <ol style="list-style-type: none"> <li>Microsoft Office Word</li> <li>Paint</li> <li>Microsoft Office Power Point</li> <li>Microsoft GIF Animator</li> </ol> </td> <td> <b>Преобразование изображений других графич. форматов, созданных в режиме True Color в формат Gif</b> <ol style="list-style-type: none"> <li>Приводит к потере качества</li> <li>Не приводит к потере качества</li> <li>Никак не влияет</li> <li>Нельзя преобразовать</li> </ol> </td> </tr> </tbody> </table> <p align="center"><small>Мой университет – www.moi-mu.ru</small></p>	Ив	Вопрос	Пв		<b>5</b>		<b>Программы, позволяющие создавать анимацию:</b>	<ol style="list-style-type: none"> <li>Microsoft Office Word</li> <li>Paint</li> <li>Microsoft Office Power Point</li> <li>Microsoft GIF Animator</li> </ol>	<b>Преобразование изображений других графич. форматов, созданных в режиме True Color в формат Gif</b> <ol style="list-style-type: none"> <li>Приводит к потере качества</li> <li>Не приводит к потере качества</li> <li>Никак не влияет</li> <li>Нельзя преобразовать</li> </ol>
Ив	Вопрос	Пв																	
	<b>4</b>																		
<b>Уменьшится или увеличится размер gif файла после сжатия его в zip архив</b>	<ol style="list-style-type: none"> <li>Вёретка газет</li> <li>Создание звуковых эффектов</li> <li>Создание анимации, баннеров</li> <li>Создание аватарки, фильма</li> </ol>	<b>Назначение Ulead Gif Animator - ...</b> <ol style="list-style-type: none"> <li>Увеличится</li> <li>Не изменится</li> <li>Уменьшится</li> <li>Нельзя сжать</li> </ol>																	
Ив	Вопрос	Пв																	
	<b>5</b>																		
<b>Программы, позволяющие создавать анимацию:</b>	<ol style="list-style-type: none"> <li>Microsoft Office Word</li> <li>Paint</li> <li>Microsoft Office Power Point</li> <li>Microsoft GIF Animator</li> </ol>	<b>Преобразование изображений других графич. форматов, созданных в режиме True Color в формат Gif</b> <ol style="list-style-type: none"> <li>Приводит к потере качества</li> <li>Не приводит к потере качества</li> <li>Никак не влияет</li> <li>Нельзя преобразовать</li> </ol>																	

IV	Вопрос	IV
	6	
<p><b>Чем сопровождается оптимизация графики</b></p> <ol style="list-style-type: none"> <li>1. Ухудшением качества</li> <li>2. Уменьшением объёма файла</li> <li>3. Всем выше перечисленным</li> <li>4. Уменьшением числа кадров</li> </ol>	<p><b>Какие форматы графических файлов поддерживает Ulead Gif Animator?</b></p> <ol style="list-style-type: none"> <li>1. Gif, Png, Swf, Avi, Mpg</li> <li>2. Wav, Mp3, Mid, Mod</li> <li>3. Cdr, Sql, Php, Cgi</li> <li>4. Gif, Wav, Swf, Avi, Cdr, Psd</li> </ol>	
Мой университет – www.moi-mu.ru		

IV	Вопрос	IV
	7	
<p><b>Панель атрибутов в Ulead Gif-аниматоре называется :</b></p> <ol style="list-style-type: none"> <li>1. Layer Panel</li> <li>2. Attributes toolbar</li> <li>3. Menu bar</li> <li>4. Central workspace</li> </ol>	<p><b>Рабочая область в Ulead Gif-аниматоре называется:</b></p> <ol style="list-style-type: none"> <li>1. Attributes toolbar</li> <li>2. Menu bar</li> <li>3. Central workspace</li> <li>4. Palette toolbar</li> </ol>	
Мой университет – www.moi-mu.ru		

IV	Вопрос	IV
	8	
<p><b>Программами 3D-анимации являются:</b></p> <ol style="list-style-type: none"> <li>1. Microsoft GIF Animator</li> <li>2. Mirage 1.5</li> <li>3. Maya</li> <li>4. TrueSpace</li> </ol>	<p><b>Программами 2D-анимации являются:</b></p> <ol style="list-style-type: none"> <li>1. Rhinoceros</li> <li>2. Moho</li> <li>3. TrueSpace</li> <li>4. Animation Stand</li> </ol>	
Мой университет – www.moi-mu.ru		

**Критерии оценки:**

○

**5 = 8 ПРАВИЛЬНЫХ ОТВЕТОВ;**

**4 = 6+7 ПРАВИЛЬНЫХ ОТВЕТОВ;**

**3 = 5 ПРАВИЛЬНЫХ ОТВЕТОВ;**

**2 = 4 И МЕНЕЕ ПРАВИЛЬНЫХ ОТВЕТОВ.**

10

**Ответы:**

○

I вариант	II вариант
1 - 1,2	1 - 1,4
2 - 2	2 - 3
3 - 4	3 - 2
4 - 3	4 - 3
5 - 3,4	5 - 4
6 - 3	6 - 4
7 - 2	7 - 3
8 - 3,4	8 - 2,4

11

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«Национальный исследовательский ядерный университет «МИФИ»  
**Димитровградский инженерно-технологический институт –**  
филиал федерального государственного автономного образовательного учреждения высшего  
образования «Национальный исследовательский ядерный университет «МИФИ»  
**(ДИТИ НИЯУ МИФИ)**



УТВЕРЖДАЮ

Директор техникума ДИТИ НИЯУ МИФИ

Н.А. Домнина

15 апреля 2021 г.

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТА  
ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ  
ПО ДИСЦИПЛИНЕ  
ОП.01 Основы информационной безопасности  
Шифр, название дисциплины**

программы подготовки специалистов среднего звена по специальности  
10.02.05 Обеспечение информационной безопасности автоматизированных  
СИСТЕМ  
Код, наименование специальности

Димитровград 2021

Методические рекомендации составлены для студентов Техникума ДИТИ НИЯУ МИФИ с целью методического сопровождения образовательного процесса; обеспечения эффективности самостоятельной работы; развития общих и профессиональных компетенций; закрепления содержания изучаемой дисциплины; развития самостоятельности в процессе решения учебных и профессиональных ситуаций; оказания методической помощи по выполнению самостоятельной работы студентами.

## СОДЕРЖАНИЕ

I.	ПОЯСНИТЕЛЬНАЯ ЗАПИСКА	4
II.	ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ	6
	- Карта самостоятельной работы студента	7
III.	ПОРЯДОК ВЫПОЛНЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОМ.	7
	- Работа с книгой	7
	- Методические рекомендации по составлению конспекта	9
	- Доклад	11
	- Методические указания по работе над рефератом	13
	- Требования к слайд-презентациям	15
	- Методические рекомендации по составлению информационного сообщения	17
	- Подготовка к практическим занятиям	17
	- Составление сводной (обобщающей) таблицы по теме	17
	- Методические рекомендации по решению задач	18
IV.	КРИТЕРИИ ОЦЕНОК РАЗЛИЧНЫХ ВИДОВ ЗАДАНИЙ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ	19

## 1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Согласно требованиям Федеральных государственных образовательных стандартов среднего профессионального образования и плана образовательного процесса колледжа каждый студент обязан выполнить по каждой учебной дисциплине определенный объем внеаудиторной самостоятельной работы.

Методические указания по выполнению внеаудиторной самостоятельной работы составлены для студентов всех специальностей среднего профессионального образования углубленной подготовки.

Методические указания по выполнению внеаудиторной самостоятельной работы по дисциплинам специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем разработаны с целью обеспечения эффективности самостоятельной работы; развития общих и профессиональных компетенций; закрепления содержания изучаемой дисциплины; применения профессиональных умений и навыков в типичных и нетипичных ситуациях; развития самостоятельности в процессе решения учебных и профессиональных ситуаций.

*Целью* методических указаний является обеспечение эффективности самостоятельной работы студентов с литературой на основе организации её изучения.

*Задачами* методических указаний по самостоятельной работе являются:

- активизация самостоятельной работы студентов;
- содействие развития творческого отношения к данной дисциплине;
- выработка умений и навыков рациональной работы с литературой;
- управление познавательной деятельностью студентов.

*Функциями* методических указаний по самостоятельной работе являются:

- определение содержания работы студентов по овладению программным материалом;
- установление требований к результатам изучения дисциплины.

Сроки выполнения и виды отчётности самостоятельной работы определяются преподавателем и доводятся до сведения студентов в начале учебного года.

В рамках освоения дисциплины студент должен продемонстрировать:

- *в области общих требований к образованности студента:*
  - понимание сущности и социальной значимости своей будущей профессии, устойчивого интереса к ней;
  - освоение профессиональной лексики
  - готовность к постоянному профессиональному росту, приобретению новых знаний, стремление к самосовершенствованию творческой самореализации;



- в области требований к уровню подготовки студента по данной дисциплине:

- умения в организации работы подразделения и собственной деятельности
- способности руководства, контроля и оценки деятельности подчиненных
- владение техниками и приемами эффективного общения

Самостоятельная работа должна содействовать активизации познавательной деятельности студентов, развитию творческого отношения к познавательной деятельности, формированию навыков самостоятельного творческого труда, умению решать профессиональные задачи, формированию потребности к непрерывному самообразованию, совершенствованию знаний и умений, расширению кругозора, приобретению опыта планирования и организации рабочего времени, выработке умений и навыков самостоятельной работы с учебной литературой, обеспечению ритмичной и качественной работы студентов в течение учебного года, снижению их загруженности в период сессии.

Данные методические указания содержат рекомендации по выполнению самостоятельной работы по указанным учебным дисциплинам, которые включают в себя:

- вид и содержание самостоятельной работы;
- задачи самостоятельной работы;
- описание последовательности выполнения задания;
- требования к оформлению работы;
- требования к форме отчетности;
- объем времени, необходимый для выполнения работы;

Контроль самостоятельной работы студентов предусматривает:

- соотнесение содержания контроля с целями обучения;
- объективность контроля;
- валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить);
- дифференциацию контрольно-измерительных материалов.

В качестве форм и методов контроля самостоятельной внеаудиторной работы студентов используются семинарские занятия, экспресс-опросы на аудиторных занятиях, самопроверка, взаимопроверка выполненного задания в группе текущий контроль выполнения, тестовые задания по разделам и темам дисциплины, рефераты и пр.

Критериями оценки результатов самостоятельной внеаудиторной работы студентов является:

- уровень освоения студентом учебного материала;
- соответствие содержания конспекта заявленной теме, верного решения к задачам;
- глубина проработки материала;
- уровень сформированности компетенций;
- правильность и полнота использования источников и др.

- уровень освоения учебного материала;
- уровень умения использовать теоретические знания при выполнении практических задач;
- уровень умения активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения материала;
- оформление материала в соответствии с требованиями;
- уровень умения четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- уровень умения определить, проанализировать альтернативные возможности, варианты действий;
- уровень умения сформулировать собственную позицию, оценку и аргументировать ее.

Организация и руководство внеаудиторной самостоятельной работой студентов осуществляется преподавателем. Внеаудиторная работа по дисциплине выполняется по заданию преподавателя, но без его непосредственного участия.

## **2. ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ**

1. Работа с книгой
2. Составление конспекта
3. Подготовка доклада
4. Подготовка и защита реферата
5. Подготовка и защита презентации
6. Подготовка к практическим занятиям
7. Подготовка информационного сообщения
8. Свободной (обобщающей) таблицы по теме
9. Решение задач

### **Карта самостоятельной работы студента**

Методические рекомендации по выполнению самостоятельной работы студентами по дисциплинам состоят из порядка выполнения самостоятельной работы студентом. Они разработаны таким образом, чтобы студенты могли самостоятельно выполнять предложенные задания, а преподаватель будет только проверять выполненные задания.

Рекомендации по выполнению самостоятельной работы помогут студентам организовать свою работу и мобилизовать себя на достижение поставленных задач. Самостоятельная работа рассчитана на разные уровни мыслительной деятельности. Выполненная работа, позволит приобрести не только знания, но и умения, навыки, а также выработать свою методику подготовки, что очень важно в дальнейшем процессе обучения.

Для выполнения самостоятельной работы студентам разрешается пользоваться учебной литературой, которая предложена в списке рекомендуемой литературы или другими источниками по усмотрению студентов.

### **3. ПОРЯДОК ВЫПОЛНЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОМ.**

#### **Работа с книгой**

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Правила самостоятельной работы с литературой:

1. Составить перечень книг, с которыми Вам следует познакомиться; «не старайтесь запомнить все, что вам в ближайшее время не понадобится, – советует студенту и молодому ученому Г. Селье, – запомните только, где это можно отыскать» Сам такой перечень должен быть систематизированным (что необходимо для семинаров, что для

экзаменов, что пригодится для написания курсовых и дипломных работ, а что Вас интересует за рамками официальной учебной деятельности, то есть что может расширить Вашу общую культуру...).

2. Обязательно выписывать все выходные данные по каждой книге (при написании курсовых и дипломных работ это позволит очень сэкономить время).

3. Разобраться для себя, какие книги (или какие главы книг) следует прочитать более внимательно, а какие – просто просмотреть.

4. При составлении перечней литературы следует посоветоваться с преподавателями (или даже с более подготовленными и эрудированными сокурсниками), которые помогут Вам лучше сориентироваться, на что стоит обратить большее внимание, а на что вообще не стоит тратить время...

5. Естественно, все прочитанные книги, учебники и статьи следует конспектировать, но это не означает, что надо конспектировать «все подряд»: можно выписывать кратко основные идеи автора и иногда приводить наиболее яркие и показательные цитаты (с указанием страниц).

6. Если книга – Ваша собственная, то допускается делать на полях книги краткие пометки или же в конце книги, на пустых страницах просто сделать свой «предметный указатель», где отмечаются наиболее интересные для Вас мысли и обязательно указываются страницы в тексте автора (это очень хороший совет, позволяющий экономить время и быстро находить «избранные» места в самых разных книгах).

7. Если Вы раньше мало работали с научной литературой, то следует выработать в себе способность «воспринимать» сложные тексты; для этого лучший прием – научиться «читать медленно», когда Вам понятно каждое прочитанное слово (а если слово незнакомое, то либо с помощью словаря, либо с помощью преподавателя обязательно его узнать), и это может занять немалое время (у кого-то – до нескольких недель и даже месяцев);

8. Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того насколько осознанно читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют четыре основные установки в чтении научного текста:

1. информационно-поисковый (задача – найти, выделить искомую информацию)
2. усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения, излагаемые автором, так и всю логику его рассуждений)
3. аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)
4. творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

#### **Методические рекомендации по составлению конспекта:**

1. Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;
2. Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;
3. Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;
4. Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;
5. Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

#### *Методические рекомендации по составлению плана-конспекта*

Такой вид изложения на бумаге создается на основе заранее составленного плана материала, состоит из определенного количества пунктов (с заголовками) и подпунктов. В процессе конспектирования каждый заголовок раскрывается – дополняется коротким текстом, в конечном итоге получается стройный план-конспект. Чем последовательнее будет план (его пункты должны максимально раскрывать содержание), тем связаннее и полноценнее будет доклад.

#### **Алгоритм подготовки плана-конспекта**

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;
2. Выделите главное, составьте план;

3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;

4. Законспектируйте материал, четко следуя пунктам плана, кратко логично организуя текст, раскрывая содержание и структуру изучаемого материала. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

#### *Методические рекомендации по составлению опорного конспекта*

Опорный конспект – это развернутый план вашего ответа на теоретический вопрос. Он призван помочь последовательно изложить тему, а преподавателю лучше понять и следить за логикой ответа.

Опорный конспект должен содержать все то, что учащийся собирает предъявить преподавателю в письменном виде. Это могут быть чертежи, графики, формулы, формулировки законов, определения, структурные схемы.

#### *Основные требования к содержанию опорного конспекта*

1. Полнота – это значит, что в нем должно быть отображено все содержание вопроса.

2. Логически обоснованная последовательность изложения.

#### *Основные требования к форме записи опорного конспекта*

1. Опорный конспект должен быть понятен не только вам, но и преподавателю.

2. По объему он должен составлять примерно один - два листа, в зависимости от объема содержания вопроса.

3. Должен содержать, если это необходимо, несколько отдельных пунктов, обозначенных номерами или пробелами.

4. Не должен содержать сплошного текста.

5. Должен быть аккуратно оформлен (иметь привлекательный вид).

#### *Алгоритм составления опорного конспекта*

1. Разбить текст на отдельные смысловые пункты.

2. Выделить пункт, который будет главным содержанием ответа.

3. Придать плану законченный вид (в случае необходимости вставить дополнительные пункты, изменить последовательность расположения пунктов).

4. Записать получившийся план в тетради в виде опорного конспекта, вставив в него все то, что должно быть, написано – определения, формулы, выводы, формулировки, выводы формул, формулировки законов и т.д.

#### **Методические рекомендации по составлению доклада**

Доклад- публичное сообщение, развёрнутое изложение какой-нибудь темы.

Доклад - вид самостоятельной научно - исследовательской работы, где автор раскрывает суть исследуемой проблемы; приводит различные точки зрения, а также собственные взгляды на нее.

Процесс работы над докладом

Чтобы облегчить вам работу над докладом, предлагаем разбить процесс на четыре последовательных этапа. Надеемся, что знакомство с ними поможет вам овладеть необходимым инструментарием и разобраться в принципах построения письменной работы. Итак, эти четыре этапа включают:

- подготовку;
- составление плана;
- написание;
- окончательное редактирование.

Подготовка. Время, которое вы посвятите данному этапу работы, предопределяет ее дальнейший ход. Тщательная подготовка вполне может рассматриваться как краеугольный камень будущего здания вашего доклада. Она позволит наиболее рациональным образом использовать имеющееся в вашем распоряжении время. В течение данного периода предстоит решить, что вы намерены писать и зачем, так что останется лишь определить для себя, как вы будете это делать. Определитесь с общими целями предстоящей работы, исходя из материалов прослушанного курса и критериев предстоящей оценки вашего труда. Просмотрите пройденный материал. Это позволит окончательно избрать предмет и наметить цели работы, а также более четко осознать уровень предъявляемых к вам требований.

Не следует забывать, что в целом написание доклада — это непрерывный процесс принятия решений. В первую очередь вам необходимо принять решение по следующим пунктам:

- выбор конкретной темы;
- цели, преследуемые вами в работе;
- критерии успешности конечного результата;
- структура и формат изложения;
- характер словаря, верный стиль, правильный тон.

Принятые решения изложите на бумаге в виде руководящих указаний и сверяйтесь с ними в ходе последующих исследований и собственно написания работы.

Планирование. Планирование — необходимый этап. Оно позволит вам обрести большую ясность и в итоге поможет сэкономить время при сборе нужной информации, при работе над материалом и написании доклада.

Вам будет проще ориентироваться в массе предстоящих дел, если вы разобьете весь процесс на ряд самостоятельных задач:

- сбор данных и их анализ могут быть структурированы по источникам или разделам будущего доклада;
- написание доклада может также происходить по разделам (собственно текстовая часть) и по средствам

графического представления материала (графики, таблицы, карты).

Кроме того, предстоит решить ряд вопросов, а именно:

- какие фактологические данные необходимы для достижения конечной цели работы?
- где почерпнуть эти данные? какой объем данных необходим?
- каким образом проводить анализ собранной информации?
- как следует расположить в докладе факты и их анализ?

Приведенная ниже последовательность действий поможет вам спланировать работу и определиться с методикой написания вашего доклада:

- определите источники необходимых вам данных (справочники и/или специальная литература);
- решите, какого характера данные по степени их уместности и достоверности вам подходят. Вы должны в полной мере понимать материал, которым оперируете;
- решите, каким образом вы будете представлять добытые сведения и свои выводы, в каком порядке они будут появляться на страницах вашего доклада, образуя его четкую и логичную структуру:
  - составьте список того, что вам предстоит сделать;
  - расположите дела в порядке очередности их выполнения;
  - составьте реальный график работы по каждому из пунктов, включая подготовку чернового варианта доклад

Техника подготовки краткого изложения состоит в следующем:

- а) прочтите весь доклад;
- б) сформулируйте его главную тему;
- в) прочтите по отдельности каждый из разделов и вычлените их основные выводы или положения;
- г) объедините пункты б) и в) в несколько логичных и взаимосвязанных формулировок.

Помните, что задачей является подготовка краткого и ясного рассказа, который дал бы полное представление о характере вашего труда; прочитайте свое краткое изложение и убедитесь, что оно верно передает содержание вашего текста и предстанет в глазах читателя самостоятельным информативным произведением.

Алгоритм подготовки доклада

1. Определите тему! Сформулируйте ее основную мысль. Уточните срок, к которому доклад (сообщение) должен быть подготовлен.



2. Подберите литературу по данному вопросу с помощью библиографических пособий, библиотечного каталога и других источников. Составьте план работы над докладом (сообщением), получите консультацию преподавателя.

3. Внимательно прочитайте источник, в котором наиболее полно раскрыта тема вашего доклада. Составьте план доклада на основе этого источника.

4. Изучите дополнительную литературу, сделайте выписки (на листах или карточках), размещая их по разделам плана.

5. Не забывайте обращаться к справочной литературе. По вопросам, которые вас затрудняют, обращайтесь за консультацией к преподавателю.

6. Подготовьте окончательный текст доклада (сообщения).

7. Приступайте к оформлению выступления:

- составьте подробный, развернутый план выступления, указывая в скобках фактический материал;
- не забывайте ссылаться на используемые источники, тщательно аргументируйте свои выводы;
- свое выступление завершите краткими выводами, которые должны оставлять у слушателей четкое представление о том, в чем вы хотели их убедить.

8. Несколько раз «проговорите» текст дома. Проконтролируйте отведенное вам время: если его окажется меньше, чем занимает выступление, сократите его, оставив только самое важное и интересное. *Нужно уважать слушателей, говорить внятно и толково, чтобы вас было интересно слушать.*

9. *Будьте готовы ответить на вопросы товарищей и защищать свою точку зрения.* Разница между докладом и сообщением — в характере переработки информации. Доклад содержит развернутое изложение, освещает вопрос преимущественно в теоретическом аспекте. Сообщение предлагает описание факта, сюжета, явления, причем довольно лаконичное.

### **Методические указания по работе над рефератом:**

Реферат - краткое изложение содержания документа или его части, научной работы, включающее основные фактические сведения и выводы, необходимые для первоначального ознакомления с источниками и определения целесообразности обращения к ним.

Современные требования к реферату - точность и объективность в передаче сведений, полнота отображения основных элементов как по содержанию, так и по форме.

Цель реферата - не только сообщить о содержании реферируемой работы, но и дать представление о вновь возникших проблемах соответствующей отрасли науки.

Реферат представляет собой краткое изложение в письменном виде или в форме публичного доклада содержания книги, учения, научного исследования и т.п.

Рефераты оцениваются по следующим основным критериями:

- актуальность содержания, высокий теоретический уровень, глубина и полнота анализа фактов, явлений, проблем, относящихся к теме;
- информационная насыщенность, новизна, оригинальность изложения вопросов; простота и доходчивость изложения;
- структурная организованность, логичность, грамматическая правильность и стилистическая выразительность;
- убедительность, аргументированность, практическая значимость и теоретическая обоснованность предложений и выводов.

Составление списка использованной литературы.

В соответствии с требованиями, предъявляемыми к реферату, докладу, необходимо составить список литературы, использованной в работе над ним.

Основные этапы работы над рефератом

В организационном плане написание реферата - процесс, распределенный во времени по этапам. Все этапы работы могут быть сгруппированы в три основные: подготовительный, исполнительский и заключительный.

Подготовительный этап включает в себя поиски литературы по определенной теме с использованием различных библиографических источников; выбор литературы в конкретной библиотеке; определение круга справочных пособий для последующей работы по теме.

Исполнительский этап включает в себя чтение книг (других источников), ведение записей прочитанного.

Заключительный этап включает в себя обработку имеющихся материалов и написание реферата, составление списка использованной литературы.

Структура реферата

Введение

Введение - это вступительная часть реферата, предваряющая текст.

Оно должно содержать следующие элементы:

- а) очень краткий анализ научных, экспериментальных или практических достижений в той области, которой посвящен реферат;
- б) общий обзор опубликованных работ, рассматриваемых в реферате;
- в) цель данной работы;
- г) задачи, требующие решения.

Объем введения при объеме реферата 10-15 может составлять одну страницу.

### Основная часть.

В основной части реферата студент дает письменное изложение материала по предложенному плану, используя материал из источников. В этом разделе работы формулируются основные понятия, их содержание, подходы к анализу, существующие в литературе, точки зрения на суть проблемы, ее характеристики.

В соответствии с поставленной задачей делаются выводы и обобщения. Очень важно не повторять, не копировать стиль источников, а выработать свой собственный, который соответствует характеру реферируемого материала.

### Заключение

Заключение подводит итог работы. Оно может включать повтор основных тезисов работы, чтобы акцентировать на них внимание читателей (слушателей), содержать общий вывод, к которому пришел автор реферата, предложения по дальнейшей научной разработке вопроса и т.п. Здесь уже никакие конкретные случаи, факты, цифры не анализируются. Заключение по объему, как правило, должно быть меньше введения.

### Список использованных источников

В строго алфавитном порядке размещаются все источники, независимо от формы и содержания: официальные материалы, монографии и энциклопедии, книги и документы, журналы, брошюры и газетные статьи.

Список использованных источников оформляется в той же последовательности, которая указана в требованиях к оформлению рефератов, курсовых, дипломных работ. (Оформление титульного листа и содержания реферата представлено в Приложениях 1,2.)

### Порядок сдачи и защиты рефератов.

Реферат сдается на проверку преподавателю за 1-2 недели до зачетного занятия.

При защите реферата преподаватель учитывает: качество степень самостоятельности студента и проявленную инициативу, связность, логичность и грамотность составления - оформление в соответствии с требованиями ГОСТ.

### Защита реферата студентом предусматривает:

- доклад по реферату не более 5-7 минут
- ответы на вопросы оппонента.
- хорошо воспринимается эмоциональное изложение материала с использованием интересных примеров;
- логика изложения позволяет слушателям лучше понять выступающего;
- употребляйте только понятные аудитории термины
- На защите запрещено чтение текста реферата.
- ваше выступление выиграет, если Вы будете максимально использовать наглядный материал.

- начните свое выступление с приветствия, огласите название вашего реферата, сформулируйте его основную идею и причину выбора темы;
- не забывайте об уважении к слушателям в течение всего выступления (не поворачивайтесь к аудитории спиной, говорите внятно);
- старайтесь ответить на все вопросы аудитории

### Требования к слайд-презентациям

В оформлении презентаций выделяют два блока: оформление слайдов и представление информации на них. Для создания качественной презентации необходимо соблюдать ряд требований, предъявляемых к оформлению данных блоков.

#### Оформление слайдов

Стиль	<ul style="list-style-type: none"> <li>• Соблюдайте единый стиль оформления</li> <li>• Избегайте стилей, которые будут отвлекать от самой презентации.</li> <li>• Вспомогательная информация (управляющие кнопки) не должны преобладать над основной информацией (текстом, иллюстрациями).</li> </ul>
Фон	Для фона предпочтительны холодные тона
Использование цвета	<ul style="list-style-type: none"> <li>• На одном слайде рекомендуется использовать не более трех цветов: один для фона, один для заголовка, один для текста.</li> <li>• Для фона и текста используйте контрастные цвета.</li> <li>• Обратите внимание на цвет гиперссылок (до и после использования).</li> <li>• Таблица сочетаемости цветов в приложении.</li> </ul>
Анимационные эффекты	<ul style="list-style-type: none"> <li>• Используйте возможности компьютерной анимации для представления информации на слайде.</li> <li>• Не стоит злоупотреблять различными анимационными эффектами, они не должны отвлекать внимание от содержания информации на слайде.</li> </ul>

#### Представление информации

Содержание информации	<ul style="list-style-type: none"> <li>• Используйте короткие слова и предложения.</li> <li>• Минимизируйте количество предлогов, наречий, прилагательных.</li> <li>• Заголовки должны привлекать внимание аудитории.</li> </ul>
Расположение информации на странице	<ul style="list-style-type: none"> <li>• Предпочтительно горизонтальное расположение информации.</li> <li>• Наиболее важная информация должна располагаться в центре экрана.</li> </ul>

	<ul style="list-style-type: none"> <li>• Если на слайде располагается картинка, надпись должна располагаться под ней.</li> </ul>
Шрифты	<ul style="list-style-type: none"> <li>• Для заголовков – не менее 24.</li> <li>• Для информации не менее 18.</li> <li>• Шрифты без засечек легче читать с большого расстояния.</li> <li>• Нельзя смешивать разные типы шрифтов в одной презентации.</li> <li>• Для выделения информации следует использовать жирный шрифт, курсив или подчеркивание.</li> <li>• Нельзя злоупотреблять прописными буквами (они читаются хуже строчных).</li> </ul>
Способы выделения информации	<p>Следует использовать:</p> <ul style="list-style-type: none"> <li>• рамки; границы, заливку;</li> <li>• штриховку, стрелки;</li> <li>• рисунки, диаграммы, схемы для иллюстрации наиболее важных фактов.</li> </ul>
Объем информации	<ul style="list-style-type: none"> <li>• Не стоит заполнять один слайд слишком большим объемом информации: люди могут одновременно запомнить не более трех фактов, выводов, определений.</li> <li>• Наибольшая эффективность достигается тогда, когда ключевые пункты отображаются по одному на каждом отдельном слайде.</li> </ul>
Виды слайдов	<p>Для обеспечения разнообразия следует использовать разные виды слайдов:</p> <ul style="list-style-type: none"> <li>• с текстом;</li> <li>• с таблицами;</li> <li>• с диаграммами.</li> </ul>

### **Подготовка к практическим занятиям**

При подготовке к практическим занятиям студентам рекомендуется:

- внимательно ознакомиться с тематикой;
- прочесть конспект лекции по теме, изучить рекомендованную литературу;
- составить краткий план ответа на каждый вопрос практического занятия;
- проверить свои знания, отвечая на вопросы для самопроверки;
- если встретятся незнакомые термины, обязательно обратиться к словарю и зафиксировать их в тетради.

### **Методические рекомендации по составлению информационного сообщения**

Информационное сообщение – это вид внеаудиторной самостоятельной работы по подготовке небольшого по объему устного сообщения для озвучивания на семинаре, практическом занятии. Сообщаемая информация носит характер уточнения или обобщения, несет новизну, отражает современный взгляд по определенным проблемам.

Сообщение отличается от докладов и рефератов не только объемом информации, но и ее характером – сообщения дополняют изучаемый вопрос фактическими или статистическими материалами. Оформляется задание письменно, оно может включать элементы наглядности (иллюстрации, демонстрацию).

Алгоритм подготовки (сообщения):

- собирать и изучить литературу по теме;
- составить план или графическую структуру сообщения;
- выделить основные понятия;
- ввести в текст дополнительные данные, характеризующие объект изучения;
- оформить текст письменно;
- сдаёт на контроль преподавателю и озвучивает в установленный срок.

### **Составление сводной (обобщающей) таблицы по теме**

Составление *сводной (обобщающей) таблицы* по теме — это вид самостоятельной работы студента по систематизации объемной информации, которая сводится (обобщается) в рамки таблицы. Формирование структуры таблицы отражает склонность студента к систематизации материала и развивает его умения по структурированию информации. Краткость изложения информации характеризует способность к ее свертыванию. В рамках таблицы наглядно отображаются как разделы одной темы (одноплановый материал), так и разделы разных тем (многоплановый материал). Такие таблицы создаются как помощь в изучении большого объема информации, желая придать ему оптимальную форму для запоминания.

Алгоритм составления *сводной (обобщающей) таблицы* :

- изучить информацию по теме;
- выбрать оптимальную форму таблицы;
- информацию представить в сжатом виде и заполнить ею основные графы таблицы;
- пользоваться готовой таблицей, эффективно подготовиться к контролю по заданной теме.

### **Методические рекомендации по решению задач**

**Задача** — это цель, заданная в определенных условиях, решение задачи — процесс достижения поставленной цели, поиск необходимых для этого средств.

Решение задачи фактически сводится к использованию

сформированного мыслительного действия, воспроизводству готового знания. Такой вид мышления называют репродуктивным.

Алгоритм решения задач:

1. Внимательно прочитайте условие задания и уясните основной вопрос, представьте процессы и явления, описанные в условии.

2. Повторно прочтите условие для того, чтобы чётко представить основной вопрос, проблему, цель решения, заданные величины, опираясь на которые можно вести поиски решения.

3. Произведите краткую запись условия задания.

4. Если необходимо составьте таблицу, схему, рисунок или чертёж.

5. Определите метод решения задания, составьте план решения.

6. Запишите основные понятия, формулы, описывающие процессы, предложенные заданной системой.

7. Найдите решение в общем виде, выразив искомые величины через заданные.

8. Проверьте правильность решения задания.

9. Произведите оценку реальности полученного решения.

10. Запишите ответ.

#### **4. КРИТЕРИИ ОЦЕНОК РАЗЛИЧНЫХ ВИДОВ ЗАДАНИЙ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ**

**Критерии и показатели, используемые при таблиц, конспектов.**

Критерии	Показатели
1. Степень заполнения и правильность ответов на поставленные вопросы Макс. - 10 баллов	- полнота раскрытия вопросов; - обоснованность способов и методов работы с материалом; - умение работать с литературой - умение обобщать, сопоставлять различные точки зрения по рассматриваемому вопросу, аргументировать основные положения и выводы.
2. Оригинальность и целостность выполнения задания Макс. - 10 баллов	- круг, полнота использования литературных источников по вопросам; - привлечение новейших работ по дизайну и оформлению творческого задания (журнальные публикации, Интернет-ресурсов и т.д.).
3. Соблюдение требований к оформлению Макс. - 5 баллов	- правильное оформление; - грамотность и культура изложения; - владение терминологией и понятийным аппаратом проблемы
4. Грамотность Макс. - 5 баллов	- отсутствие орфографических и синтаксических ошибок;

	<ul style="list-style-type: none"> <li>- отсутствие опечаток, сокращений слов, кроме общепринятых;</li> <li>- литературный стиль.</li> </ul>
--	--

Конвертация полученных баллов в оценку:

- 27 – 30 баллов – «отлично»;
- 26 – 22 баллов – «хорошо»;
- 21 – 17 баллов – «удовлетворительно»;
- менее 17 баллов – «неудовлетворительно»

### **Критерии и показатели, используемые при оценивании учебного реферата, доклада**

Оценивание реферата, доклада: знания и умения на уровне требований стандарта дисциплины: знание фактического материала, усвоение общих представлений, понятий, идей.

Степень обоснованности аргументов и обобщений (полнота, глубина, всесторонность раскрытия темы, логичность и последовательность изложения материала, корректность аргументации и системы доказательств, характер и достоверность примеров, иллюстративного материала, широта кругозора автора, наличие знаний интегрированного характера, способность к обобщению).

Качество и ценность полученных результатов (степень завершенности реферативного исследования, спорность или однозначность выводов).

Критерии	Показатели
1. Новизна реферированного текста Макс. - 10 баллов	<ul style="list-style-type: none"> <li>- новизна и самостоятельность в рассмотрении темы,</li> <li>- наличие авторской позиции, самостоятельность суждений.</li> </ul>
2. Степень раскрытия сущности проблемы Макс. - 20 баллов	<ul style="list-style-type: none"> <li>- соответствие плана теме реферата, доклада;</li> <li>- соответствие содержания теме и плану;</li> <li>- полнота и глубина раскрытия основных понятий, определений;</li> <li>- обоснованность способов и методов работы с материалом;</li> <li>- умение работать с литературой, систематизировать и структурировать материал;</li> <li>- умение обобщать, сопоставлять различные точки зрения по рассматриваемому вопросу, аргументировать основные положения и выводы.</li> </ul>
3. Обоснованность выбора источников Макс. - 5 баллов	<ul style="list-style-type: none"> <li>- круг, полнота использования литературных источников по проблеме;</li> <li>- привлечение новейших работ по проблеме (журнальные публикации, материалы сборников научных трудов и т.д.).</li> </ul>



4. Соблюдение требований к оформлению Макс. -5 баллов	- правильное оформление ссылок на используемую литературу; - грамотность и культура изложения; - владение терминологией и понятийным аппаратом проблемы; - соблюдение требований к объему реферата; - культура оформления: выделение абзацев.
5. Грамотность Макс. - 5 баллов	- отсутствие орфографических и синтаксических ошибок, стилистических погрешностей; отсутствие опечаток, сокращений слов, кроме общепринятых.

Конвертация полученных баллов в оценку:

Реферат следующим образом:

- 42 – 45 баллов – «отлично»;
- 41– 37 баллов – «хорошо»;
- 36– 30 баллов – «удовлетворительно»;
- мене 30 баллов – «неудовлетворительно».

Баллы учитываются в процессе текущей оценки знаний программного материала.

Данное задание выполняется при изучении учебной литературы, нормативной, используя записи в конспекте, электронное учебное пособие, ресурсы сети Интернет.

### Критерии оценивания сообщения

Параметры оценки	Максимальное количество баллов
<b>Содержание сообщения</b>	
Материал представлен четко и ясно	5
Тема раскрыта полностью	10
Материал отвечает на направляющие вопросы	10
Имеется список использованных ресурсов	5
Отсутствие орфографических ошибок	5

31-35 – «отлично»

26-30 – «хорошо»

21-25 – «удовлетворительно»

менее 21 баллов – «неудовлетворительно»

### Критерии оценивания учебной презентации

Параметры оценки	Максимальное количество баллов
<b>Содержание презентации</b>	
Материал представлен четко и ясно	5

Тема раскрыта полностью	10
Материал отвечает на направляющие вопросы	10
Имеется список использованных ресурсов	5
Отсутствие орфографических ошибок	5
<b>Дизайн</b>	
Презентация оформлена красиво	5
Текст хорошо читается	5
Цветовое решение гармонично	5
Использование диаграмм, графиков, таблиц	5
Иллюстрации не отвлекают внимание от содержания	5
Организация работы	
Четкое планирование работы группы	10
Оправданные способы общения во время работы	5
Соблюдение авторских прав	5
Общее количество баллов	100

90-100 – «отлично»

89-80 – «хорошо»

79-60 – «удовлетворительно»

менее 60 баллов – «неудовлетворительно»

### Критерии оценивания решения задач

Параметры оценки	Максимальное количество баллов
<b>Содержание сообщения</b>	
Правильность алгоритма решения	10
Правильность расчетов	10
Правильность оформления	10

27-30 – «отлично»

23-26 – «хорошо»

19-22 – «удовлетворительно»

менее 19 баллов – «неудовлетворительно»

**Образец оформления титульного листа реферата**

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«Национальный исследовательский ядерный университет «МИФИ»  
**Димитровградский инженерно-технологический институт –**  
филиал федерального государственного автономного образовательного учреждения высшего  
образования «Национальный исследовательский ядерный университет «МИФИ»  
**(ДИТИ НИЯУ МИФИ)**

**РЕФЕРАТ**

**по теме:** \_\_\_\_\_  
наименование темы  
**дисциплина**            **«Основы информационной безопасности»**

Разработал:  
студент (ка) гр № \_\_\_\_\_  
Отделения \_\_\_\_\_  
\_\_\_\_\_  
(Ф.И.О.)

Проверил:  
преподаватель  
\_\_\_\_\_

Димитровград, 202\_\_

**Образец оформления содержания реферата**

**СОДЕРЖАНИЕ**

Введение	3
.....	
Основная часть	4
.....	
Заключение	9
.....	
Список литературы	10
.....	

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«Национальный исследовательский ядерный университет «МИФИ»  
**Димитровградский инженерно-технологический институт –**  
филиал федерального государственного автономного образовательного учреждения высшего  
образования «Национальный исследовательский ядерный университет «МИФИ»  
**(ДИТИ НИЯУ МИФИ)**



## ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине  
**ОП.01 Основы информационной безопасности**  
программы подготовки специалистов среднего звена по специальности  
10.02.05 Обеспечение информационной безопасности автоматизированных  
систем

код, наименование специальности

Форма обучения очная

Учебный цикл ОП

Разработчик фонда оценочных средств:  
Н.А. Шульга, преподаватель техникума ДИТИ НИЯУ МИФИ

Димитровград 2021

ФОС составлен на основе ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Минобрнауки РФ от 9 декабря 2016 г. № 1553 и ПООП, разработанной ФУМО в системе СПО по укрупненной группе специальностей 10.00.00 «Информационная безопасность», зарегистрированной в федеральном реестре примерных основных образовательных программ, регистрационный № 10.02.05-170703 от 03/07/2017 (Протокол № 1 от 28.03.2017)

Рассмотрен  
на заседании методической цикловой комиссии  
Информационных технологий  
Протокол № 8 от 26.03 2021 г.  
Председатель МЦК Г.М. Глек

## **СОДЕРЖАНИЕ**

### **1. Паспорт фонда оценочных средств**

1.1. Область применения

### **2. Методика контроля успеваемости и оценивания результатов освоения программы дисциплины**

2.1 Перечень компетенций, формируемых в процессе изучения дисциплины

2.2 Общая процедура и сроки оценочных мероприятий. Оценка освоения программы.

### **3. Комплект материалов для оценки освоенных знаний и умений**

3.1 Текущий контроль

3.2 Промежуточная аттестация

3.3 Методика формирования результирующей оценки по дисциплине.

## 1. Паспорт фонда оценочных средств

Фонд оценочных средств предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины ОП.01 Основы информационной безопасности.

Фонд оценочных средств разработан в соответствии с требованиями ФГОС

- 10.02.05 Обеспечение информационной безопасности автоматизированных систем и рабочей программой учебной дисциплины ОП.01 Основы информационной безопасности».

## 2. Методика контроля успеваемости и оценивания результатов освоения программы дисциплины

### 2.1 Перечень компетенций, формируемых в процессе изучения дисциплины Перечень компетенций с указанием этапов (уровней) их формирования

Планируемые результаты освоения ОПОП (индикаторы достижения компетенции)	Результаты обучения по дисциплине
Общие компетенции (ОК)	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	
Знать: возможные траектории профессионального развития и самообразования Уметь: определять актуальность нормативно-правовой документации в профессиональной деятельности Владеть: навыками определения актуальности нормативно-правовой документации в профессиональной деятельности.	Знать: возможные траектории профессионального развития и самообразования Уметь: определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития Владеть: навыками определения актуальности нормативноправовой документации в профессиональной деятельности; выстраивания траектории профессионального и личностного развития
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	



<p>Знать: сущность гражданско- патриотической позиции, общечеловеческие ценности, правила поведения в ходе выполнения профессиональной деятельности</p> <p>Уметь: описывать значимость своей профессии, презентовать структуру профессиональной деятельности по специальности.</p> <p>Владеть: навыками представления структуры профессиональной деятельности по специальности</p>	<p>Знать: сущность гражданско- патриотической позиции, общечеловеческие ценности, правила поведения в ходе выполнения профессиональной деятельности.</p> <p>Уметь: описывать значимость своей профессии, презентовать структуру профессиональной деятельности по специальности.</p> <p>Владеть: навыками творческого представления структуры профессиональной деятельности по специальности.</p>
<p>ОК 09. Использовать информационные технологии в профессиональной деятельности.</p>	
<p>Знать: современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности.</p> <p>Уметь: применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение</p> <p>Владеть: навыками применения средств информационных технологий для решения профессиональных задач.</p>	<p>Знать: современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности.</p> <p>Уметь: применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение.</p> <p>Владеть: навыками применения средств информационных технологий для решения профессиональных задач; использования</p>
<p>ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.</p>	

<p>Знать: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения.</p> <p>Уметь: понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые).</p> <p>Владеть: навыками понимания общего смысла четко произнесенных высказываний на известные темы (профессиональные и бытовые), на базовые профессиональные темы; участия в диалогах на знакомые общие и профессиональные темы; построения простых высказываний о себе и о своей профессиональной деятельности; обоснования и объяснения своих действий (текущих и планируемых).</p>	<p>Знать: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности.</p> <p>Уметь: понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы.</p> <p>Владеть: навыками понимания общего смысла четко произнесенных высказываний на известные темы (профессиональные и бытовые), на базовые профессиональные темы; участия в диалогах на знакомые общие и профессиональные темы; построения простых высказываний о себе и о своей профессиональной деятельности; обоснования и объяснения своих действий (текущих и планируемых); письма простых связных сообщений на знакомые или интересующие профессиональные темы.</p>
--	--

Профессиональные компетенции (ПК)

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации

## **2.2 Общая процедура и сроки оценочных мероприятий. Оценка освоения программы.**

Оценивание результатов обучения студентов по дисциплине ОП.01 Основы информационной безопасности осуществляется по регламенту текущего контроля и промежуточной аттестации.

Текущий контроль в семестре проводится с целью обеспечения своевременной обратной связи, для коррекции обучения, активизации самостоятельной работы студентов. Формы текущего контроля знаний: - устный опрос; - письменный опрос; - тестирование; - выполнение и защита практических работ; - выполнение практических заданий. Проработка конспекта лекций и учебной литературы осуществляется студентами в течение всего семестра, после изучения новой темы. Защита практических производится студентом в день их выполнения в соответствии с планом-графиком. Преподаватель проверяет правильность выполнения практической работы студентом, контролирует знание студентом пройденного материала с помощью контрольных вопросов или тестирования. Оценка компетентности осуществляется следующим образом: по окончании выполнения задания студенты оформляют отчет, который затем выносится на защиту. В процессе защиты выявляется информационная компетентность в соответствии с заданием на практической работы, затем преподавателем дается комплексная оценка деятельности студента. Высокую оценку получают студенты, которые при подготовке материала для самостоятельной работы сумели самостоятельно составить логический план к теме и реализовать его, собрать достаточный фактический материал, показать связь рассматриваемой темы с современными проблемами науки и общества, со специальностью студента и каков авторский вклад в систематизацию, структурирование материала. Оценка качества подготовки на основании выполненных заданий ведется преподавателям (с обсуждением результатов), баллы начисляются в зависимости от сложности задания. Для определения фактических оценок каждого показателя выставляются следующие баллы Фактические баллы за ответ на теоретический блок - от 0 до 50 баллов Подготовка и участие в практических занятиях - от 0 до 30 баллов. Подготовка доклада и презентации - от 0 до 20 баллов. Студентам, пропустившим занятия и не ответившим по темам занятий, общий балл по текущему контролю снижается на 10% за каждый час пропуска занятий. Студентам, проявившим активность во время практических занятий, общий балл по текущему контролю может быть увеличен на 1015%. Оценка качества подготовки по результатам самостоятельной работы студента ведется: 1) преподавателем - оценка глубины проработки материала, рациональность и содержательная ёмкость представленных интеллектуальных продуктов, наличие креативных элементов, подтверждающих самостоятельность суждений по теме; 2) группой - в ходе обсуждения представленных материалов; 3) студентом лично - путем самоанализа достигнутого уровня понимания темы Итоговый контроль освоения умения и усвоенных знаний дисциплины ОП.01 Основы информационной безопасности осуществляется на зачетном занятии.

**Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания**

Уровень освоения компетенции	Планируемые результаты обучения (в соотв. с уровнем освоения компетенции)	Критерии оценивания результатов обучения				
		1	2	3	4	5
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.	Неудовлетворительная оценка выставляется студенту, который не знает программный материал, допускает существенные ошибки, не выполняет практические работы.	Неудовлетворительная оценка выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.	Удовлетворительная оценка выставляется студенту, если он имеет знания только основного материала, допускает неточности, испытывает затруднения при выполнении практических работ.	Хорошая оценка выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, правильно применяет теоретические положения при решении практических вопросов и задач.	Отличная оценка выставляется студенту, если он глубоко и прочно усвоил программный материал, свободно справляется с задачами, вопросами и другими видами применения знаний, владеет разносторонним и навыками и приемами выполнения практических задач.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	Неудовлетворительная оценка выставляется студенту, который не знает программный материал, допускает существенные ошибки, не выполняет практические работы.	Неудовлетворительная оценка выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.	Удовлетворительная оценка выставляется студенту, если он имеет знания только основного материала, допускает неточности, испытывает затруднения при выполнении практических работ.	Хорошая оценка выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, правильно применяет теоретические положения при решении практических вопросов и задач.	Отличная оценка выставляется студенту, если он глубоко и прочно усвоил программный материал, свободно справляется с задачами, вопросами и другими видами применения знаний, владеет разносторонним и навыками и приемами выполнения практических задач.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.	Неудовлетворительная оценка выставляется студенту, который не знает программный материал, допускает существенные ошибки, не выполняет практические работы.	Неудовлетворительная оценка выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.	Удовлетворительная оценка выставляется студенту, если он имеет знания только основного материала, допускает неточности, испытывает затруднения при выполнении практических работ.	Хорошая оценка выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, правильно применяет теоретические положения при решении практических вопросов и задач.	Отличная оценка выставляется студенту, если он глубоко и прочно усвоил программный материал, свободно справляется с задачами, вопросами и другими видами применения знаний, владеет разносторонним и навыками и приемами выполнения практических задач.

ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.	Неудовлетворительная оценка выставляется студенту, который не знает программный материал, допускает существенные ошибки, не выполняет практические работы.	Неудовлетворительная оценка выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.	Удовлетворительная оценка выставляется студенту, если он имеет знания только основного материала, допускает неточности, испытывает затруднения при выполнении практических работ.	Хорошая оценка выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, правильно применяет теоретические положения при решении практических вопросов и задач.	Отличная оценка выставляется студенту, если он глубоко и прочно усвоил программный материал, свободно справляется с задачами, вопросами и другими видами применения знаний, владеет разносторонним и навыками и приемами выполнения практических задач.
ПК 2.4. информации ограниченного доступа.	Осуществлять обработку, хранение и передачу который не знает программный материал, допускает существенные ошибки, не выполняет практические работы.	Неудовлетворительная оценка выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.	Неудовлетворительная оценка выставляется студенту, он имеет знания только основного материала, допускает неточности, испытывает затруднения при выполнении практических работ.	Удовлетворительная оценка выставляется студенту, если материал, грамотно и по существу излагает его, правильно применяет теоретические положения при решении практических вопросов и задач.	Хорошая оценка выставляется студенту, если он твердо знает прочно усвоил программный материал, свободно справляется с задачами, вопросами и другими видами применения знаний, владеет разносторонним и навыками и приемами выполнения практических задач	Отличная оценка выставляется студенту, если он глубоко и

### 3 Комплект материалов для оценки освоенных умений и усвоенных знаний

#### 3.1 Текущий контроль

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

1. Определение объектов защиты на типовом объекте информатизации (по вариантам)
2. Классификация защищаемой информации по видам тайны и степеням конфиденциальности (по вариантам).
3. Определение угроз объекта информатизации и их классификация (по вариантам)
4. Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности (по вариантам)
5. Выбор мер защиты информации для автоматизированного рабочего места (по вариантам)

#### 3.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине проводится в форме устного опроса по пройденным темам. (Зачетное занятие - это итоговое проверочное испытание.) Оценка может быть выставлена по рейтингу текущего контроля, если он не ниже 60. Зачетное занятие проводится по расписанию сессии.

1. Понятие информации и информационной безопасности.
2. Информация, сообщения, информационные процессы как объекты информационной безопасности.
3. Обзор защищаемых объектов и систем.

4. Понятие «угроза информации». Понятие «риска информационной безопасности».
5. Примеры преступлений в сфере информации и информационных технологий.
6. Сущность функционирования системы защиты информации.
7. Защита человека от опасной информации и от неинформированности в области информационной безопасности.
8. Целостность, доступность и конфиденциальность информации.
9. Классификация информации по видам тайны и степеням конфиденциальности.
10. Понятия государственной тайны и конфиденциальной информации.
11. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.
12. Цели и задачи защиты информации.
13. Основные понятия в области защиты информации.
14. Элементы процесса менеджмента ИБ.
15. Модель интеграции информационной безопасности в основную деятельность организации.
16. Понятие Политики безопасности.
17. Понятие угрозы безопасности информации
18. Системная классификация угроз безопасности информации
19. Каналы и методы несанкционированного доступа к информации
20. Уязвимости. Методы оценки уязвимости информации
21. Анализ существующих методик определения требований к защите информации
22. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации
23. Виды мер и основные принципы защиты информации
24. Организационная структура системы защиты информации
25. Законодательные акты в области защиты информации
26. Российские и международные стандарты, определяющие требования к защите информации
27. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации
28. Основные механизмы защиты информации.
29. Система защиты информации.
30. Меры защиты информации, реализуемые в автоматизированных (информационных) системах
31. Программные и программно-аппаратные средства защиты информации
32. Инженерная защита и техническая охрана объектов информатизации
33. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим.
34. Принципы построения организационно-распорядительной системы

#### **Типовые задания**

1. Определение объектов защиты на типовом объекте информатизации (по вариантам)
2. Классификация защищаемой информации по видам тайны и степеням конфиденциальности (по вариантам).

## 3.3

## Методика формирования результирующей оценки по дисциплине.

Баллы	Оценка экзамена	Требования к знаниям
5	«отлично»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал дополнительной литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
4	«хорошо»	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
3	«удовлетворительно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.
2	«неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.



**ЛИСТ РЕГИСТРАЦИИ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ**  
**в УМК учебной дисциплины (МДК, ПМ) \_\_\_\_\_**  
**на 20\_\_\_\_-20\_\_\_\_\_ учебный год**

Специальность: \_\_\_\_\_

Форма обучения: \_\_\_\_\_

№	Наименование материала	Дополнения и изменения
1.	Рабочая программа дисциплины (модуля)	
2.	Календарно-тематический план учебной дисциплины (модуля)	
3.	Планы учебных занятий (по усмотрению преподавателя)	
4.	Методические рекомендации по выполнению практических и/или лабораторных работ (инструкционные карты)	
5.	Методические рекомендации по организации самостоятельной работы студентов	
6.	Методические рекомендации по курсовому (дипломному) проектированию	
7.	Методические рекомендации по применению инновационных образовательных технологий и методов обучения в преподавании учебной дисциплины	
8.	Фонд оценочных средств (контрольно-измерительные материалы для учебной дисциплины, контрольно-оценочные средства для модуля)	

Дополнения и изменения внес: \_\_\_\_\_

\_\_\_\_\_

ФИО, должность

подпись

УМК учебной дисциплины (МДК, ПМ) рассмотрено и одобрено на заседании МЦК

\_\_\_\_\_

Протокол № \_\_\_\_ от \_\_\_\_\_ г.

Председатель МЦК \_\_\_\_\_ / \_\_\_\_\_ /