

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
федеральное государственное автономное образовательное учреждение высшего  
образования  
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 33

УТВЕРЖДАЮ

Руководитель направления

проф., д.т.н., доц.

(должность, уч. степень, звание)

С.В. Беззатеев

(инициалы, фамилия)



(подпись)

«25» мая 2023 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Методология защиты информации»

(Наименование дисциплины)

Код направления подготовки/ специальности	10.03.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности	Безопасность компьютерных систем
Форма обучения	очная

Санкт-Петербург– 2023



## Аннотация

Дисциплина «Методология защиты информации» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 10.03.01 «Информационная безопасность» направленности «Безопасность компьютерных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-3 «Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств защиты информации, способен к использованию и внедрению результатов исследований»

Содержание дисциплины охватывает круг вопросов, связанных с изучением методов, теоретических и практических основ обеспечения информационной безопасности в автоматизированных информационных системах.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельная работа студента.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме зачета.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский»

## 1. Перечень планируемых результатов обучения по дисциплине

### 1.1. Цели преподавания дисциплины

Цель преподавания дисциплины – изучение методов, теоретических и практических основ обеспечения информационной безопасности в автоматизированных информационных системах.

1.2. Дисциплина входит в состав части, формируемой участниками образовательных отношений, образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Профессиональные компетенции	ПК-3 Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств защиты информации, способен к использованию и внедрению результатов исследований	ПК-3.3.1 знает методы и средства планирования и организации исследований и разработок ПК-3.3.2 знает методы анализа научных данных ПК-3.У.1 умеет применять актуальную нормативную документацию в соответствующей области знаний ПК-3.В.1 владеет навыками организации сбора и изучения научно-технической информации по теме исследований и разработок ПК-3.В.2 владеет навыками анализа научных данных, результатов экспериментов и наблюдений

## 2. Место дисциплины в структуре ОП

Дисциплина может базироваться на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- «Криптографическая защита информации»,
- «Программно-аппаратная защита информации»,

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и могут использоваться при изучении других дисциплин:

- «Управление информационной безопасностью»,
- «Преддипломная практика».

## 3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
--------------------	-------	---------------------------

		№7
1	2	3
<b>Общая трудоемкость дисциплины, ЗЕ/ (час)</b>	3/ 108	3/ 108
<b>Из них часов практической подготовки</b>	34	34
<b>Аудиторные занятия, всего час.</b>	51	51
в том числе:		
лекции (Л), (час)	17	17
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	34	34
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		
<b>Самостоятельная работа, всего (час)</b>	57	57
<b>Вид промежуточной аттестации:</b> зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Зачет	Зачет

Примечание: \*\* кандидатский экзамен

#### 4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.

Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 7					
Раздел 1. Автоматизированная информационная система как объект защиты	2	4			7
Раздел 2. Требования информационной безопасности АИС	4	12			16
Раздел 3. Методы защиты информации	6	10			16
Раздел 4. Средства защиты информации	5	8			18
Итого в семестре:	17		34		57
Итого	17	0	34	0	57

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
<b>1</b>	Тема 1.1. Архитектура «клиент-сервер» АИС. Тема 1.2. Модели нарушителя и угроз АИС
<b>2</b>	Тема 2.1. Общие требования к построению защищенной

	<p>АИС.</p> <p>Тема 2.2. Требования к подсистеме аутентификации и управления доступом.</p> <p>Тема 2.3. Требования к подсистемам криптографической защиты информации и антивирусной защиты.</p> <p>Тема 2.4. Требования к подсистемам резервирования /восстановления информации, контроля эталонного состояния информации и рабочей среды.</p> <p>Тема 2.5. Требования к подсистеме управления безопасностью</p>
<b>3</b>	<p>Тема 3.1. Многоуровневая модель защиты информации в АИС на архитектуре «клиент-сервер».</p> <p>Тема 3.2. Методы защиты информации на физическом уровне модели OSI.</p> <p>Тема 3.3. Методы защиты информации на канальном уровне модели OSI. Тема 3.4. Методы защиты информации на сеансовом уровне модели OSI. Тема 3.5. Методы защиты информации на транспортном уровне модели OSI.</p> <p>Тема 3.6. Методы защиты информации на сеансовом уровне модели OSI.</p> <p>Тема 3.7. Методы защиты информации на прикладном уровне модели OSI.</p>
<b>4</b>	<p>Тема 4.1. Средства защиты информации от несанкционированного доступа.</p> <p>Тема 4.2. Средства защиты информации от вредоносного кода.</p> <p>Тема 4.3. Средства защиты информации от межсетевых воздействий.</p> <p>Тема 4.4. Средства криптографической защиты информации.</p>

#### 4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено					
Всего					

#### 4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 7				
1	Требования к построению защищенной АИС и ее элементов	8		2
2	Многоуровневая модель защиты информации в АИС на архитектуре «клиент-сервер»	8		3
3	Методы защиты информации на уровнях модели OSI	10		3
4	Средства защиты информации	8		4
Всего		34		

4.5. Курсовое проектирование/ выполнение курсовой работы  
Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся  
Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 7, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	37	37
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	5	5
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	15	15
Всего:	57	57

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)  
Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 7-11.

6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004/М 87- 604316- ED	Мошак Н. Н. Защищенные инфотелекоммуникации. Анализ и синтез [Электронный ресурс]: монография / Н. Н. Мошак; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - СПб.: Изд-во ГУАП, 2014. - 197 с.	50
004 М 87	Организация безопасного доступа к информационным ресурсам: учебное пособие / Н. Н. Мошак, Т. М. Татарникова. - СПб.: Изд-во ГУАП, 2014. - 121 с	40
X404.3 М 48	Информационная безопасность и защита информации: учебное пособие/ В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред. С. А Клейменов. - 5-е изд., стер. - М.: Академия, 2011. - 331 с.	25
004 Ш 22	Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для СПО / В. Ф. Шаньгин. - М.: ФОРУМ: ИНФРА-М, 2016. - 416 с.	10
	Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. <a href="http://znanium.com/catalog.php?bookinfo=474838">http://znanium.com/catalog.php?bookinfo=474838</a>	

#### 7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
<a href="http://www.intuit.ru/studies/courses/10/10/info">http://www.intuit.ru/studies/courses/10/10/info</a>	Владимир Галатенко. Основы информационной безопасности (курс лекций, с дистанционным обучением)

#### 8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
-------	--------------



	Не предусмотрено
--	------------------

8.2. Перечень информационно-справочных систем, используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

## 9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Аудитория для проведения практических занятий	

## 10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Зачет	Список вопросов; Тесты; Задачи.

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
«отлично» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся глубоко и всесторонне усвоил программный материал;</li> <li>– уверенно, логично, последовательно и грамотно его излагает;</li> <li>– опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления;</li> <li>– умело обосновывает и аргументирует выдвигаемые им идеи;</li> <li>– делает выводы и обобщения;</li> <li>– свободно владеет системой специализированных понятий.</li> </ul>

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
«хорошо» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы;</li> <li>– не допускает существенных неточностей;</li> <li>– увязывает усвоенные знания с практической деятельностью направления;</li> <li>– аргументирует научные положения;</li> <li>– делает выводы и обобщения;</li> <li>– владеет системой специализированных понятий.</li> </ul>
«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы;</li> <li>– допускает несущественные ошибки и неточности;</li> <li>– испытывает затруднения в практическом применении знаний направления;</li> <li>– слабо аргументирует научные положения;</li> <li>– затрудняется в формулировании выводов и обобщений;</li> <li>– частично владеет системой специализированных понятий.</li> </ul>
«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> <li>– обучающийся не усвоил значительной части программного материала;</li> <li>– допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении;</li> <li>– испытывает трудности в практическом применении знаний;</li> <li>– не может аргументировать научные положения;</li> <li>– не формулирует выводов и обобщений.</li> </ul>

### 10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
	Учебным планом не предусмотрено	

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
1	<ol style="list-style-type: none"> <li>1. Дайте определение понятию информационная безопасность.</li> <li>2. Перечислите основные составляющие информационной безопасности.</li> <li>3. Какое значение имеют составляющие информационной безопасности для субъектов информационных отношений?</li> <li>4. Каковы интересы РФ в информационной сфере?</li> <li>5. Определите источники угроз информационной безопасности РФ и постройте их классификацию.</li> <li>6. Перечислите основные методы обеспечения информационной безопасности РФ.</li> </ol>	ПК-3.3.1
2	<ol style="list-style-type: none"> <li>7. Какие основные проблемы международного сотрудничества стоят на повестке дня сегодня?</li> <li>8. Перечислите основные документы в области международной информационной безопасности.</li> <li>9. Каково, на ваш взгляд, положение дел в области МИБ сегодня?</li> </ol>	ПК-3.3.2

	10. Проанализируйте различные определения понятия «защита информации» и «информационная безопасность». 11. Дайте определение понятию защита информации.	
3	12. Что понимается под термином безопасность информации? 13. Что включает в себя защита информации? 14. Какие цели преследует защита информации?	ПК-3.У.1
4	15. Какое место занимает защита информации в информационной безопасности? 16. Какие уровни задействованы в обеспечении информационной безопасности?	ПК-3.В.1
5	17. Что представляет собой политика безопасности организации? 18. Что входит в анализ рисков? 19. Что представляет собой программа безопасности организации? 20. Определите предмет защиты информации. 21. Сформулируйте основные свойства информации. 22. Дайте определение конфиденциальной информации. 23. Перечислите уровни секретности государственной тайны. 24. Раскройте сущность основных подходов к измерению количества информации. 25. Раскройте сущность информации как объекта права собственности. 7. Раскройте сущность объекта защиты. 26. Составьте классификацию угроз информационной безопасности. 27. Раскройте основные группы классификации. 28. На основании чего строится модель нарушителя информационной безопасности? 29. Сформулируйте основные принципы построения системы защиты информации. 30. Перечислите основные модели защиты информации и их особенности. 31. В чем заключается сущность методов защиты от случайных угроз? 32. Дайте определение понятиям идентификации и аутентификации. 33. Перечислите основные виды аутентификации. 34. В чем заключается повышение надежности и отказоустойчивости информационных систем? 35. Какую роль играет подготовленность персонала в построении системы защиты информации? 36. Какие методы и средства используются для организации противодействия традиционным методам шпионажа и диверсий? 37. Раскройте особенность построения защиты от несанкционированного доступа 38. Какие методы защиты информации относятся к криптографическим?	ПК-3.В.2

Перечень тем для курсового проектирования/выполнения курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для курсового проектирования/выполнения курсовой работы

№ п/п	Примерный перечень тем для курсового проектирования/выполнения курсовой работы
-------	--

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	<p>Правильный вариант ответа отмечен знаком +</p> <p>1) К правовым методам, обеспечивающим информационную безопасность, относятся:</p> <ul style="list-style-type: none"> <li>- Разработка аппаратных средств обеспечения правовых данных</li> <li>- Разработка и установка во всех компьютерных правовых сетях журналов учета действий</li> <li>+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности</li> </ul> <p>2) Основными источниками угроз информационной безопасности являются все указанное в списке:</p> <ul style="list-style-type: none"> <li>- Хищение жестких дисков, подключение к сети, инсайдерство</li> <li>+ Перехват данных, хищение данных, изменение архитектуры системы</li> <li>- Хищение данных, подкуп системных администраторов, нарушение регламента работы</li> </ul> <p>3) Виды информационной безопасности:</p> <ul style="list-style-type: none"> <li>+ Персональная, корпоративная, государственная</li> <li>- Клиентская, серверная, сетевая</li> <li>- Локальная, глобальная, смешанная</li> </ul> <p>4) Цели информационной безопасности – своевременное обнаружение, предупреждение:</p> <ul style="list-style-type: none"> <li>+ несанкционированного доступа, воздействия в сети</li> <li>- инсайдерства в организации</li> <li>- чрезвычайных ситуаций</li> </ul> <p>5) Основные объекты информационной безопасности:</p> <ul style="list-style-type: none"> <li>+ Компьютерные сети, базы данных</li> <li>- Информационные системы, психологическое состояние пользователей</li> <li>- Бизнес-ориентированные, коммерческие системы</li> </ul> <p>6) Основными рисками информационной безопасности являются:</p> <ul style="list-style-type: none"> <li>- Искажение, уменьшение объема, перекодировка информации</li> <li>- Техническое вмешательство, выведение из строя оборудования сети</li> <li>+ Потеря, искажение, утечка информации</li> </ul> <p>7) К основным принципам обеспечения информационной безопасности относится:</p> <ul style="list-style-type: none"> <li>+ Экономической эффективности системы безопасности</li> <li>- Многоплатформенной реализации системы</li> <li>- Усиления защищенности всех звеньев системы</li> </ul> <p>8) Основными субъектами информационной безопасности являются:</p> <ul style="list-style-type: none"> <li>- руководители, менеджеры, администраторы компаний</li> <li>+ органы права, государства, бизнеса</li> <li>- сетевые базы данных, фаерволлы</li> </ul> <p>9) К основным функциям системы безопасности можно отнести все перечисленное:</p> <ul style="list-style-type: none"> <li>+ Установление регламента, аудит системы, выявление рисков</li> <li>- Установка новых офисных приложений, смена хостинг-компании</li> <li>- Внедрение аутентификации, проверки контактных данных пользователей</li> </ul> <p>тест 10) Принципом информационной безопасности является принцип недопущения:</p>	

<p>+ Неоправданных ограничений при работе в сети (системе)</p> <ul style="list-style-type: none"> <li>- Рисков безопасности сети, системы</li> <li>- Презумпции секретности</li> </ul> <p>11) Принципом политики информационной безопасности является принцип:</p> <ul style="list-style-type: none"> <li>+ Невозможности миновать защитные средства сети (системы)</li> <li>- Усиления основного звена сети, системы</li> <li>- Полного блокирования доступа при риск-ситуациях</li> </ul> <p>12) Принципом политики информационной безопасности является принцип:</p> <ul style="list-style-type: none"> <li>+ Усиления защищенности самого незащищенного звена сети (системы)</li> <li>- Перехода в безопасное состояние работы сети, системы</li> <li>- Полного доступа пользователей ко всем ресурсам сети, системы</li> </ul> <p>13) Принципом политики информационной безопасности является принцип:</p> <ul style="list-style-type: none"> <li>+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)</li> <li>- Одноуровневой защиты сети, системы</li> <li>- Совместимых, однотипных программно-технических средств сети, системы</li> </ul> <p>14) К основным типам средств воздействия на компьютерную сеть относятся:</p> <ul style="list-style-type: none"> <li>- Компьютерный сбой</li> <li>+ Логические закладки («мины»)</li> <li>- Аварийное отключение питания</li> </ul> <p>15) Когда получен спам по e-mail с приложенным файлом, следует:</p> <ul style="list-style-type: none"> <li>- Прочитать приложение, если оно не содержит ничего ценного – удалить</li> <li>- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама</li> <li>+ Удалить письмо с приложением, не раскрывая (не читая) его</li> </ul> <p>16) Принцип Кирхгофа:</p> <ul style="list-style-type: none"> <li>- Секретность ключа определена секретностью открытого сообщения</li> <li>- Секретность информации определена скоростью передачи данных</li> <li>+ Секретность закрытого сообщения определяется секретностью ключа</li> </ul> <p>17) ЭЦП – это:</p> <ul style="list-style-type: none"> <li>- Электронно-цифровой преобразователь</li> <li>+ Электронно-цифровая подпись</li> <li>- Электронно-цифровой процессор</li> </ul> <p>18) Наиболее распространены угрозы информационной безопасности корпоративной системы:</p> <ul style="list-style-type: none"> <li>- Покупка нелегального ПО</li> <li>+ Ошибки эксплуатации и неумышленного изменения режима работы системы</li> <li>- Сознательного внедрения сетевых вирусов</li> </ul> <p>19) Наиболее распространены угрозы информационной безопасности сети:</p> <ul style="list-style-type: none"> <li>- Распределенный доступ клиент, отказ оборудования</li> <li>- Моральный износ сети, инсайдерство</li> <li>+ Сбой (отказ) оборудования, нелегальное копирование данных</li> </ul> <p>тест_20) Наиболее распространены средства воздействия на сеть офиса:</p> <ul style="list-style-type: none"> <li>- Слабый трафик, информационный обман, вирусы в интернет</li> <li>+ Вирусы в сети, логические мины (закладки), информационный перехват</li> <li>- Компьютерные сбои, изменение администрирования, топологии</li> </ul> <p>21) Утечкой информации в системе называется ситуация, характеризующаяся:</p> <ul style="list-style-type: none"> <li>+ Потерей данных в системе</li> <li>- Изменением формы информации</li> </ul>	
--	--

	<ul style="list-style-type: none"> <li>- Изменением содержания информации</li> <li>22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются: <ul style="list-style-type: none"> <li>+ Целостность</li> <li>- Доступность</li> <li>- Актуальности</li> </ul> </li> <li>23) Угроза информационной системе (компьютерной сети) – это: <ul style="list-style-type: none"> <li>+ Вероятное событие</li> <li>- Детерминированное (всегда определенное) событие</li> <li>- Событие, происходящее периодически</li> </ul> </li> <li>24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется: <ul style="list-style-type: none"> <li>- Регламентированной</li> <li>- Правовой</li> <li>+ Защищаемой</li> </ul> </li> <li>25) Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке: <ul style="list-style-type: none"> <li>+ Программные, технические, организационные, технологические</li> <li>- Серверные, клиентские, спутниковые, наземные</li> <li>- Личные, корпоративные, социальные, национальные</li> </ul> </li> <li>26) Окончательно, ответственность за защищенность данных в компьютерной сети несет: <ul style="list-style-type: none"> <li>+ Владелец сети</li> <li>- Администратор сети</li> <li>- Пользователь сети</li> </ul> </li> <li>27) Политика безопасности в системе (сети) – это комплекс: <ul style="list-style-type: none"> <li>+ Руководств, требований обеспечения необходимого уровня безопасности</li> <li>- Инструкций, алгоритмов поведения пользователя в сети</li> <li>- Нормы информационного права, соблюдаемые в сети</li> </ul> </li> <li>28) Наиболее важным при реализации защитных мер политики безопасности является: <ul style="list-style-type: none"> <li>- Аудит, анализ затрат на проведение защитных мер</li> <li>- Аудит, анализ безопасности</li> <li>+ Аудит, анализ уязвимостей, риск-ситуаций</li> </ul> </li> </ul>	
--	--	--

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

#### 11. Методические указания для обучающихся по освоению дисциплины

Формирование профессиональной компетентности на основе системы теоретических и методологических знаний и специальных умений в области информационной безопасности и их использования в профессиональной деятельности будущего специалиста. В курсе рассматривается основной понятийный аппарат информационной безопасности.

## **Методические указания для обучающихся по освоению лекционного материала**

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

### Планируемые результаты при освоении обучающимся лекционного материала:

- получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;
- получение опыта творческой работы совместно с преподавателем;
- развитие профессионально–деловых качеств, любви к предмету и самостоятельного творческого мышления.
- появление необходимого интереса, необходимого для самостоятельной работы;
- получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;
- научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);
- получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

### Структура предоставления лекционного материала:

- Изложение лекционного материала;
- Представление теоретического материала преподавателем в виде слайдов;
- Освоение теоретического материала по практическим вопросам;
- Список вопросов по теме для самостоятельной работы студента (Табл.21).

## **Методические указания для обучающихся по прохождению лабораторных работ**

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

- приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;
- закрепление, развитие и детализация теоретических знаний, полученных на лекциях;
- получение новой информации по изучаемой дисциплине;
- приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

### **Задание и требования к проведению лабораторных работ**

Задание на лабораторные работы представлены по темам изучаемой дисциплины и представляют собой реализацию изучаемых задач:

Рассмотрение и анализ доктрины информационной безопасности российской федерации

Необходимо проанализировать Доктрину ИБ РФ и построить схему органов государственной власти и самоуправления, отвечающих за информационную безопасность и определить их функциональные обязанности; определить положения государственной политики в области обеспечения ИБ, выделить первоочередные мероприятия по обеспечению ИБ, дать им оценку.

Определение целей защиты информации на предприятии регионального уровня

Необходимо проанализировать структуру местного предприятия, рассмотреть виды информации и носители, используемые в его подразделениях. Сформулировать цели защиты информации на данном предприятии. Составить программу информационной безопасности

Рассмотрение особенностей объекта защиты информации

Используя данные предыдущей практической работы, рассмотреть особенности каждого типа носителей информации, отметить плюсы и минусы каждого типа, условия хранения и обработки.

Определение угроз информационной безопасности и анализ рисков на предприятии

Исходя из целей защиты информации и носителей информации, выявленных на предыдущих занятиях, необходимо определить список угроз ИБ, характерных для данного предприятия. Проанализировать риски, определить степень их допустимости. Составить модели нарушителей информационной безопасности, актуальных для данного предприятия.

Построение концепции безопасности предприятия

Определите, комплекс практических мероприятий, направленных на обеспечение информационной безопасности предприятия. Составьте программу информационной безопасности предприятия.

### **Структура и форма отчета о лабораторной работе**

Отчёт по лабораторной работе оформляется индивидуально каждым студентом, выполнившим необходимые (независимо от того, выполнялся ли эксперимент индивидуально или в составе группы студентов). Страницы отчёта следует пронумеровать (титульный лист не нумеруется, далее идет страница 2 и т.д.). Титульный лист отчёта должен содержать фразу: «Отчёт по лабораторной работе «Название работы», чуть ниже: Выполнил студент группы (номер группы) (Фамилия, инициалы)». Внизу листа следует указать текущий год. Например, Отчёт по лабораторной работе № (номер работы) «Введение в спектральный анализ», Выполнил студент группы 5221 Иванов И.И. Вторая страница текста, следующая за титульным листом, должна начинаться с пункта: Цель работы. Отчёт, как правило, должен содержать следующие основные разделы:

1. Цель работы;
2. Теоретическая часть;
3. Программное обеспечение, используемое в работе;
4. Результаты;
5. Выводы.

В случае необходимости в конце отчёта приводится перечень литературы.

### **Требования к оформлению отчета о лабораторной работе**

Теоретическая часть должна содержать минимум необходимых теоретических сведений о предметной области. Не следует копировать целиком или частично методическое пособие (описание) лабораторной работы или разделы учебника.



В разделе Программное обеспечение необходимо описать, с помощью каких инструментальных средств и каким образом были разработаны модели и получены результаты. Рисунки, блок-схемы, описание модели и её особенностей, необходимость отладки – все это должно быть представлено в указанном разделе.

Раздел Результаты включает в себя скриншоты программного приложения, полученные при выполнении лабораторной работы. Рисунки, графики и таблицы нумеруются и подписываются заголовками.

Выводы не должны быть простым перечислением того, что сделано. Здесь важно отметить, какие новые знания о предмете исследования были получены при выполнении работы, к чему привело обсуждение результатов, насколько выполнена заявленная цель работы. Выводы по работе каждый студент делает самостоятельно. В случае необходимости в конце отчёта приводится Список литературы, использованной при подготовке к работе. В тексте отчёта делаются краткие ссылки на литературу (учебники, справочники, иные источники...) номером в квадратных скобках, напр., [1]. Литературные источники нумеруются по мере их появления в тексте отчёта. В конце отчёта даётся их подробный список. На все источники списка литературы должны быть ссылки в тексте отчёта, там, где это необходимо.

При сдаче отчёта преподаватель может сделать устные и письменные замечания, задать дополнительные вопросы. Все ответы на дополнительные вопросы, обсуждения выполняются студентом на отдельных листах, включаемых в отчёт (при этом в тексте основного отчёта делается сноска или другой значок, которому будет соответствовать новый материал). При этом письменные замечания преподавателя должны остаться в тексте для ясности динамики работы над отчётом.

Объём отчёта должен быть оптимальным для понимания того, что и как сделал студент, выполняя работу. Обязательные требования к отчёту включают общую и специальную грамотность изложения, а также аккуратность оформления.

После приёма преподавателем отчёт хранится на кафедре.

### **Методические указания для обучающихся по прохождению самостоятельной работы**

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

### **Методические указания для обучающихся по прохождению промежуточной аттестации**

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

– зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

– дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой