

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

Кафедра № 33

УТВЕРЖДАЮ  
Ответственный за образовательную  
программу  
\_\_\_\_\_  
доц., к.э.н., доц.  
(должность, уч. степень, звание)

\_\_\_\_\_  
Т.Н. Елина  
(инициалы, фамилия)  
\_\_\_\_\_  
(подпись)  
«19» февраля 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Инженерно-технические средства 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
Год приема	2025

Лист согласования рабочей программы дисциплины

Программу составил (а)

\_\_\_\_\_  
к.т.н., доц.  
(должность, уч. степень, звание)

\_\_\_\_\_  
19.02.2025  
(подпись, дата)

\_\_\_\_\_  
В.С. Коломойцев  
(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«19» февраля 2025 г, протокол № 7

Заведующий кафедрой № 33

\_\_\_\_\_  
д.т.н., доц.  
(уч. степень, звание)

\_\_\_\_\_  
19.02.2025  
(подпись, дата)

\_\_\_\_\_  
С.В. Беззатеев  
(инициалы, фамилия)

Заместитель директора института №3 по методической работе

\_\_\_\_\_  
(должность, уч. степень, звание)

\_\_\_\_\_  
(подпись, дата)

\_\_\_\_\_  
Н.В. Решетникова  
(инициалы, фамилия)

## Аннотация

Дисциплина «Инженерно-технические средства 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»

ПК-5 «Способен организовывать и проводить настройку программных, программно-аппаратных (в том числе крипто-графических) и технических средств и систем защиты от несанкционированного доступа»

ПК-6 «Способен администрировать средства защиты информации прикладного и системного программного обеспечения»

Содержание дисциплины охватывает круг вопросов, связанных с анализом возможных угроз информационной безопасности объектов информатизации, преимущественно связанных с возможными утечками информации. Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа студента.

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

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

Цели преподавания дисциплины состоят в получении знаний и умений по выбору средств технической защиты информации, пригодных для выполнения заданных функций в комплексной системе защиты информации объекта, комплексированию, определению оптимальных режимов работы и организации их эксплуатации в подсистеме инженерно-технической защиты информации..

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.У.1 умеет применять актуальную нормативную документацию в соответствующей области знаний
Профессиональные компетенции	ПК-5 Способен организовывать и проводить настройку программных, программно-аппаратных (в том числе крипто-графических) и технических средств и систем защиты от несанкционированного доступа	ПК-5.У.1 умеет устанавливать и настраивать параметры сетевых протоколов, реализованных в телекоммуникационном оборудовании
Профессиональные компетенции	ПК-6 Способен администрировать	ПК-6.3.2 знает принципы построения антивирусного программного обеспечения

	средства защиты информации прикладного и системного программного обеспечения	ПК-6.В.1 владеет определением порядка установки программного обеспечения с целью соблюдения требований по защите информации ПК-6.В.2 владеет навыками по выполнению работ по обнаружению вредоносного программного обеспечения
--	--	---

## 2. Место дисциплины в структуре ОП

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

- «Основы информационной безопасности»,
- «Информатика»,
- «Основы теории информации»

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

- «НТР»,
- «ГИА»

## 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)	36	36
<b>Самостоятельная работа, всего (час)</b>	21	21
<b>Вид промежуточной аттестации:</b> зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Экз.	Экз.

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					
Введение					
Раздел 1. Обобщенная структура канала передачи информации	2				2
Раздел 2. Средства обработки информации. Защита от утечек и потерь информации.	2		34		2
Раздел 3. Оптический канал.	2				2
Раздел 4. Звуковой канал.	2				3
Текущий контроль	1				
Раздел 5. Каналы проводной связи.	2				4
Раздел 6. Каналы беспроводной связи	2				4
Раздел 7. Порядок и средства проведения контроля защищенности. Заключение	2				4
Итого в семестре:	17		34		21
Итого	17	0	34	0	21

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>	Введение. Требования к системе защиты информации. Содержание учебной дисциплины, порядок изучения. Основная и дополнительная литература.
<b>2</b>	Раздел 1. Обобщенная структура канала передачи информации. Каналы утечки информации. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Меры, препятствующие утечке информации.
<b>3</b>	Раздел 2. Средства обработки информации. Защита от утечек и потерь информации. Особенности использования компьютера как средства подготовки, передачи, получения и хранения информации. Съем информации с компьютера. Режимы работы компьютера.
<b>4</b>	Раздел 3. Оптический канал. Информация, распространяющаяся по оптическому каналу. Характерные особенности канала. Оптические приборы, используемые для получения информации, их характеристики. Преобразования оптического сигнала. Фиксация оптической информации. Защита от утечек информации.
<b>5</b>	Раздел 4. Звуковой канал. Защита от утечек информации. Характеристики информации, передаваемой по звуковому каналу. Приборы и преобразователи, используемые для получения и накопления информации, их характеристики и особенности функционирования. Способы защиты от утечек информации
<b>6</b>	Раздел 5. Каналы проводной связи. Устройство, функционирование

	и съем информации с телефона. Понятие о длинных линиях. Подключение к линиям проводной связи, способы его обнаружения. Защита от утечек информации
<b>7</b>	Раздел 6 Каналы беспроводной связи. Защита от утечек информации. Диапазоны радиоволн, особенности их распространения. Функции ГКРЧ. Структура, функционирование разведприемника. BYOD (Bring Your Own Devices) и средства защиты от них
<b>8</b>	Раздел 7. Порядок и средства проведения контроля защищенности. Заключение

#### 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	Устройство и безопасная эксплуатация компьютера	4	4	22
2	Виртуальная машина VirtualBox и ее использование	4	4	2
3	Live DVD системного администратора	4	4	2
4	Базовая система ввода-вывода IBM PC	4	4	2
5	Структура FAT и NTFS. Удаление/восстановление файла	4	4	2
6	Резервное копирование информации	4	4	2
7	Устройства отображения информации	4	4	2
8	Защита отчетов, обсуждение результатов	6	6	2
Всего		34	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)	9	9
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	2	2
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	10	10
Всего:	21	21

#### 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	Защищенные инфотелекоммуникации. Анализ и синтез [Текст] : монография / Н. Н. Мошак ; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2014. - 197 с.	40
004 М 87	Организация безопасного доступа к информационным ресурсам [Текст] : учебное пособие / Н. Н. Мошак, Т. М. Татарникова ; С.- Петерб. гос. ун-т аэрокосм. приборостроения. -СПб. : Изд-во ГУАП, 2014. - 121 с.	40
004 В 75	Основы защиты информации [Текст] : учебное пособие / А. В. Воронов, Н. В. Волошина ; С.- Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2009. - 78 с	74
004.056.5(075)	Железняк, В. К. Защита информации от	102

Ж 51	утечки по техническим каналам. - СПб.: ГОУ ВПО "СПбГУАП", 2006.	
	<a href="http://e.lanbook.com/view/book/1122/">http://e.lanbook.com/view/book/1122/</a> Шаньгин В.Ф. Защита компьютерной информации. ДМК Пресс, 2010. - 544 стр.	
	<a href="http://znanium.com/bookread2.php?book=169345">http://znanium.com/bookread2.php?book=169345</a> Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с.	
	<a href="http://znanium.com/bookread2.php?book=453862">http://znanium.com/bookread2.php?book=453862</a> Аверченков, В. И. Организационная защита информации [электронный ресурс] : учеб. пособие для вузов / В. И. Аверченков, М. Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2011. – 184 с.	

#### 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
	Не предусмотрено

#### 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 таблице12.

Таблица 12 – Состав материально-технической базы



№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Лаборатория технической защиты информации Специализированная мебель; технические средства обучения, служащие для представления учебной информации большой аудитории; лабораторное оборудование (ПЭВМ - 10 шт., объединенных в локальную вычислительную сеть с выходом в вычислительную сеть ГУАП и Интернет)	Б.М. 14-34

#### 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
Экзамен	Список вопросов к экзамену; Экзаменационные билеты; Задачи; Тесты.

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 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	– обучающийся глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	– обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий.

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
«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
1	Требования к системе защиты информации. Каналы утечки информации. ГОСТ Р 51275-2006 Защита информации.	ПК-3.У.1
2	Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Меры, препятствующие утечке информации. Особенности использования компьютера как средства подготовки, передачи, получения и хранения информации.	ПК-5.У.1
3	Съем информации с компьютера. Режимы работы компьютера. Защита от утечек информации в оптическом канале. Способы защиты от утечек информации в звуковом канале.	ПК-6.3.2
4	Защита от утечек информации в каналах проводной связи. Защита от утечек информации в каналах беспроводной связи.	ПК-6.В.1
5	Структура, функционирование разведприемника. BYOD (Bring Your Own Devices) и средства защиты от них Порядок и средства проведения контроля защищенности.	ПК-6.В.2

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
	Учебным планом не предусмотрено	

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
	Учебным планом не предусмотрено

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><b>1. Кто является основным ответственным за определение уровня классификации информации?</b></p> <p>А. Руководитель среднего звена  В. Высшее руководство  С. Владелец  D. Пользователь</p> <p><b>2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?</b></p> <p>А. Сотрудники  В. Хакеры  С. Атакующие  D. Контрагенты (лица, работающие по договору)</p> <p><b>3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?</b></p> <p>А. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования  В. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации  С. Улучшить контроль за безопасностью этой информации  D. Снизить уровень классификации этой информации</p> <p><b>4. Что самое главное должно продумать руководство при классификации данных?</b></p> <p>А. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным  В. Необходимый уровень доступности, целостности и конфиденциальности  С. Оценить уровень риска и отменить контрмеры  D. Управление доступом, которое должно защищать данные</p> <p><b>5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?</b></p> <p>А. Владельцы данных  В. Пользователи  С. Администраторы  D. Руководство</p> <p><b>6. Что такое процедура?</b></p> <p>А. Правила использования программного и аппаратного обеспечения в компании  В. Пошаговая инструкция по выполнению задачи  С. Руководство по действиям в ситуациях, связанных с</p>	

	<p>безопасностью, но не описанных в стандартах</p> <p>D. Обязательные действия</p> <p><b>7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?</b></p> <p>A. Поддержка высшего руководства</p> <p>B. Эффективные защитные меры и методы их внедрения</p> <p>C. Актуальные и адекватные политики и процедуры безопасности</p> <p>D. Проведение тренингов по безопасности для всех сотрудников</p> <p><b>8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?</b></p> <p>A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски</p> <p>B. Когда риски не могут быть приняты во внимание по политическим соображениям</p> <p>C. Когда необходимые защитные меры слишком сложны</p> <p>D. Когда стоимость контрмер превышает ценность актива и потенциальные потери</p> <p><b>9. Что такое политики безопасности?</b></p> <p>A. Пошаговые инструкции по выполнению задач безопасности</p> <p>B. Общие руководящие требования по достижению определенного уровня безопасности</p> <p>C. Широкие, высокоуровневые заявления руководства</p> <p>D. Детализированные документы по обработке инцидентов безопасности</p> <p><b>10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?</b></p> <p>A. Анализ рисков</p> <p>B. Анализ затрат / выгоды</p> <p>C. Результаты ALE</p> <p>D. Выявление уязвимостей и угроз, являющихся причиной риска</p> <p><b>11. Что лучше всего описывает цель расчета ALE?</b></p> <p>A. Количественно оценить уровень безопасности среды</p> <p>B. Оценить возможные потери для каждой контрмеры</p> <p>C. Количественно оценить затраты / выгоды</p> <p>D. Оценить потенциальные потери от угрозы в год</p> <p><b>12. Тактическое планирование – это:</b></p> <p>A. Среднесрочное планирование</p> <p>B. Долгосрочное планирование</p> <p>C. Ежедневное планирование</p> <p>D. Планирование на 6 месяцев</p> <p><b>13. Что является определением воздействия (exposure) на безопасность?</b></p> <p>A. Нечто, приводящее к ущербу от угрозы</p> <p>B. Любая потенциальная опасность для информации или систем</p> <p>C. Любой недостаток или отсутствие информационной безопасности</p> <p>D. Потенциальные потери от угрозы</p> <p><b>14. Эффективная программа безопасности требует сбалансированного применения:</b></p> <p>A. Технических и нетехнических методов</p> <p>B. Контрмер и защитных механизмов</p> <p>C. Физической безопасности и технических средств защиты</p>	
--	--	--

D. Процедур безопасности и шифрования

**15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:**

A. Внедрение управления механизмами безопасности

B. Классификацию данных после внедрения механизмов безопасности

C. Уровень доверия, обеспечиваемый механизмом безопасности

D. Соотношение затрат / выгод

**16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?**

A. Только военные имеют настоящую безопасность

B. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности

C. Военным требуется больший уровень безопасности, т.к. их риски существенно выше

D. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

**17. Как рассчитать остаточный риск?**

A. Угрозы x Риски x Ценность актива

B. (Угрозы x Ценность актива x Уязвимости) x Риски

C.  $SLE \times Частота = ALE$

D. (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля

**18. Что из перечисленного не является целью проведения анализа рисков?**

A. Делегирование полномочий

B. Количественная оценка воздействия потенциальных угроз

C. Выявление рисков

D. Определение баланса между воздействием риска и стоимостью необходимых контрмер

**19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?**

A. Поддержка

B. Выполнение анализа рисков

C. Определение цели и границ

D. Делегирование полномочий

**20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?**

A. Чтобы убедиться, что проводится справедливая оценка

B. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ

C. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа

D. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

	<p><b>21. Что является наилучшим описанием количественного анализа рисков?</b></p> <p>A. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности</p> <p>B. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков</p> <p>C. Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков</p> <p>D. Метод, основанный на суждениях и интуиции</p> <p><b>22. Почему количественный анализ рисков в чистом виде не достижим?</b></p> <p>A. Он достижим и используется</p> <p>B. Он присваивает уровни критичности. Их сложно перевести в денежный вид.</p> <p>C. Это связано с точностью количественных элементов</p> <p>D. Количественные измерения должны применяться к качественным элементам</p> <p><b>23. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?</b></p> <p>A. Много информации нужно собрать и ввести в программу</p> <p>B. Руководство должно одобрить создание группы</p> <p>C. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки</p> <p>D. Множество людей должно одобрить данные</p> <p><b>24. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?</b></p> <p>A. Стандарты</p> <p>B. Должный процесс (Due process)</p> <p>C. Должная забота (Due care)</p> <p>D. Снижение обязательств</p> <p><b>25. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?</b></p> <p>A. Список стандартов, процедур и политик для разработки программы безопасности</p> <p>B. Текущая версия ISO 17799</p> <p>C. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях</p> <p>D. Открытый стандарт, определяющий цели контроля</p>	
--	---	--

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

### 11.1. 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 обучающимися 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:

Введение. Требования к системе защиты информации. Содержание учебной дисциплины, порядок изучения. Основная и дополнительная литература.

Раздел 1. Обобщенная структура канала передачи информации.

Раздел 2. Средства обработки информации. Защита от утечек и потерь информации.

Раздел 3. Оптический канал.

Раздел 4. Звуковой канал.

Раздел 5. Каналы проводной связи.

Раздел 6 Каналы беспроводной связи.

Раздел 7. Порядок и средства проведения контроля защищенности.

Заключение

### 11.2. Методические указания для обучающихся по выполнению лабораторных работ (если предусмотрено учебным планом по данной дисциплине)

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 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.

Структура и форма отчета о лабораторной работе. Отчет о лабораторной работе должен включать в себя: титульный лист, формулировку задания, теоретические положения, используемые при выполнении лабораторной работы, описание процесса выполнения лабораторной работы, полученные результаты и выводы. Требования к оформлению отчета о лабораторной работе. По каждой лабораторной работе выполняется отдельный отчет. Титульный лист оформляется в соответствии с шаблоном (образцом) приведенным на сайте ГУАП ([www.guap.ru](http://www.guap.ru)) в разделе «Сектор нормативной документации». Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями, приведенными на сайте ГУАП ([www.guap.ru](http://www.guap.ru)) в разделе «Сектор нормативной документации». Методические указания по прохождению лабораторных работ: Методические указания к лабораторным работам по дисциплине «Техническая защита информации» - электронный ресурс кафедры No33.

### 11.3. 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).

### 11.4. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

### 11.5. 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».



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