

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

Кафедра № 25

УТВЕРЖДАЮ

Руководитель образовательной программы

\_\_\_\_\_  
доц., к.т.н., доц.

(должность, уч. степень, звание)

\_\_\_\_\_  
Н.В. Марковская

(инициалы, фамилия)

\_\_\_\_\_  
(подпись)

«24» июня 2024 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита информационных процессов в компьютерных системах»  
(Наименование дисциплины)

Код направления подготовки/ специальности	11.03.02
Наименование направления подготовки/ специальности	Инфокоммуникационные технологии и системы связи
Наименование направленности	Программно-защищенные инфокоммуникации
Форма обучения	очная
Год приема	2024

Лист согласования рабочей программы дисциплины

Программу составил (а)

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

\_\_\_\_\_  
(подпись, дата)

24.06.2024

\_\_\_\_\_  
А.А. Овчинников  
(инициалы, фамилия)

Программа одобрена на заседании кафедры № 25  
«24» июня 2024 г, протокол № 12/2023-24

Заведующий кафедрой № 25

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

\_\_\_\_\_  
(подпись, дата)

24.06.2024

\_\_\_\_\_  
А.М. Тюрликов  
(инициалы, фамилия)

Заместитель директора института №2 по методической работе

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

\_\_\_\_\_  
(подпись, дата)

24.06.2024

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

## Аннотация

Дисциплина «Защита информационных процессов в компьютерных системах» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 11.03.02 «Инфокоммуникационные технологии и системы связи» направленности «Программно-защищенные инфокоммуникации». Дисциплина реализуется кафедрой «№25».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-1 «Способен к развитию систем и сетей передачи данных»

ПК-2 «Способен осуществлять экспериментальные испытания, мониторинг состояния и проверку качества работы, проведение измерений и диагностику ошибок и отказов телекоммуникационного оборудования, сетевых устройств, программного обеспечения инфокоммуникаций»

ПК-4 «Способен оценивать параметры безопасности и защищать программное обеспечение и сетевые устройства администрируемой сети с помощью специальных средств управления безопасностью»

ПК-6 «Способен к администрированию средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)»

Содержание дисциплины охватывает круг вопросов, связанных с изучением методов, механизмов и средств защиты информации в процессе ее обработки, хранения и передачи в компьютерных системах с учетом возможных угроз и требований нормативных документов.

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 зачета.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа.

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Цели преподавания дисциплины состоят в изучении методов, механизмов и средств защиты информации в процессе ее обработки, хранения и передачи в компьютерных системах с учетом возможных угроз и требований нормативных документов.

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-1 Способен к развитию систем и сетей передачи данных	ПК-1.3.6 знать методы анализа и обобщения отечественного и международного опыта в области систем и сетей передачи данных
Профессиональные компетенции	ПК-2 Способен осуществлять экспериментальные испытания, мониторинг состояния и проверку качества работы, проведение измерений и диагностику ошибок и отказов телекоммуникационного оборудования, сетевых устройств, программного обеспечения инфокоммуникаций	ПК-2.3.2 знать способы настройки сетевого оборудования, изменения конфигурации и установки новых релизов программного обеспечения ПК-2.3.3 знать правила работы с различными информационными системами и базами данных ПК-2.3.4 знать правила информационной безопасности при работе с телекоммуникационным оборудованием ПК-2.У.1 уметь проводить анализ конфигурации и параметров сети доступа и оборудования
Профессиональные компетенции	ПК-4 Способен оценивать параметры безопасности и защищать программное обеспечение и сетевые устройства администрируемой сети с помощью специальных средств управления безопасностью	ПК-4.3.2 знать основные принципы, криптографические протоколы и программные средства обеспечения информационной безопасности сетевых устройств ПК-4.3.3 знать основы защиты информации и базовые угрозы ПК-4.У.1 уметь применять программные, аппаратные и программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа ПК-4.У.2 уметь пользоваться нормативно-технической документацией в области обеспечения информационной безопасности инфокоммуникационных систем ПК-4.У.3 уметь определять требования и

		возможные решения в области защиты информации совместно со специалистами по информационной безопасности ПК-4.В.1 владеть навыками и средствами установки и управления специализированными программными средствами защиты сетевых устройств администрируемой сети от несанкционированного доступа
Профессиональные компетенции	ПК-6 Способен к администрированию средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	ПК-6.У.1 уметь подключать и настраивать современные средства обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов); работать с контрольно-измерительными аппаратными и программными средствами ПК-6.В.1 владеть навыками установки дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризации

## 2. Место дисциплины в структуре ОП

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

- «Корпоративная защита от внутренних угроз информационной безопасности»,
- «Производственная практика»

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

- «Производственная 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
		№8
1	2	3
<b>Общая трудоемкость дисциплины, ЗЕ/ (час)</b>	2/ 72	2/ 72
<b>Из них часов практической подготовки</b>	20	20
<b>Аудиторные занятия, всего час.</b>	30	30
в том числе:		
лекции (Л), (час)	10	10
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	20	20
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		

<b>Самостоятельная работа</b> , всего (час)	42	42
<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 8					
Раздел 1. Введение	1				
Раздел 2. Анализ возможных угроз в компьютерных системах.	2		2		8
Раздел 3. Особенности защиты информационного процесса хранения данных	2		4		8
Текущий контроль	1				10
Раздел 4. Особенности защиты информационного процесса обработки данных	2		2		8
Раздел 5. Особенности защиты информационного процесса передачи данных	2		12		8
Итого в семестре:	10		20		42
Итого	10	0	20	0	42

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. Понятие информационного процесса. Классификация информационных процессов. Основные виды защищаемой информации. Тема 1.2. Понятие угрозы информационному процессу. Классификация угроз информационным процессам. Требования к защите данных в компьютерных системах
<b>2</b>	Тема 2.1. Компьютерные системы и обеспечение их безопасности Архитектура сложных компьютерных систем с точки зрения обеспечения их безопасности Тема 2.2. Угрозы в компьютерных системах Основные угрозы информации в компьютерных системах. Специфика возникновения угроз в компьютерных сетях. Тема 2.3. Уязвимости в компьютерных системах Способы и средства анализа уязвимостей в компьютерных системах. Классификация компьютерных систем по возможным уязвимостям

	<p>Тема 2.4. Каналы утечки информации в компьютерных системах</p> <p>Тема 2.5. Атаки на различных уровнях открытых систем.</p> <p>Возможности атаки на различных уровнях открытых систем.</p> <p>Аппаратные средства обеспечения безопасности открытых систем</p> <p>Тема 2.6. Алгоритмы проведения анализа и оценки угроз.</p>
3	<p>Тема 3.1. Характеристика и состав процесса хранения данных</p> <p>Системы хранения данных, архитектуры хранения данных, физические компоненты систем хранения данных. RAID-массивы. Интеллектуальные системы хранения данных. Сети хранения данных</p> <p>Тема 3.2. Резервное копирование и восстановление</p> <p>Цель резервного копирования. Восстановление после отказа. Операционное резервное копирование. Архивирование.</p> <p>Тема 3.3. Репликация</p> <p>Локальная репликация. Технологии локальной репликации: на основе хоста, на основе массива хранения данных. Удаленная репликация. Режимы удаленной репликации. Технологии удаленной репликации: на основе хоста, на основе массива хранения данных, на основе SAN.</p> <p>Тема 3.4. Безопасность инфраструктуры хранения.</p> <p>Триада риска: активы, угрозы, уязвимости. Домены безопасности хранения. Безопасность области доступа к приложению: контроль доступа пользователя к данным, защита инфраструктуры хранения, шифрование данных.</p> <p>Безопасность области управления доступом: контроль административного доступа, защита инфраструктуры управления.</p> <p>Безопасность резервного копирования, восстановления и архивов.</p> <p>Тема 3.5. Внедрение безопасности в сети хранения.</p> <p>Архитектура безопасности SAN. Основные механизмы безопасности SAN.</p> <p>Тема 3.6. Мониторинг инфраструктуры хранения.</p> <p>Параметры для мониторинга. Мониторинг компонентов. Мониторинг доступности. Мониторинг безопасности.</p>
4	<p>Тема 4.1. Характеристика и состав процесса обработки данных</p> <p>Схема процесса обработки данных, угрозы и уязвимости процесса</p> <p>Примеры процессов обработки данных.</p> <p>Тема 4.2. Базовые технологии обеспечения безопасности процесса обработки данных.</p> <p>Кодирование данных. Программные закладки. Защита от изучения. Защита программ от несанкционированного копирования. Защита исполняемых файлов.</p> <p>Тема 4.3. Защита программ и данных в операционной системе Windows</p> <p>Тема 4.4. Защита программ и данных в операционных системах семейства Unix</p>
5	<p>Тема 5.1. Характеристика и состав процесса передачи данных</p> <p>Архитектура процесса передачи данных. Угрозы и уязвимости процесса.</p> <p>Типичные проблемы безопасности в глобальных сетях на примере Интернет и локальных сетей предприятий.</p> <p>Тема 5.2. Базовые технологии обеспечения безопасности процесса передачи данных.</p> <p>Средства защиты информации в открытых сетях. Защита данных на канальном уровне. Защита данных на сетевом уровне.</p> <p>Тема 5.3. Основы построения виртуальных частных сетей</p> <p>Варианты технической реализации: на базе межсетевых экранов, маршрутизаторов, программного обеспечения, сетевой ОС,</p>

	специализированных аппаратных средств. Тема 5.4. Межсетевые экраны Функции и назначение межсетевых экранов. Создание демилитаризованной зоны. Схемы подключения межсетевых экранов.
--	---

#### 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 8				
1	Формирование модели угроз в информационной системе	2	2	2
2	Криптографическая защита данных на логических и физических дисках	2	2	3
3	Защита виртуальных дисков	2	2	3
4	Анализ и мониторинг возможных угроз в операционной системе Windows	2	2	4
5	Организация защищенного канала связи	2	2	5
6	Методы ограничения доступа к ресурсам АС	2	2	5
7	Настройка политики безопасности межсетевого экрана	2	2	5
8	Аттестация автоматизированных систем. Методика контроля	2	2	5
9	Реализация технологии виртуальных частных сетей	4	4	5
Всего		20	20	

#### 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 8, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	22	22
Подготовка к текущему контролю успеваемости (ТКУ)	10	10
Подготовка к промежуточной аттестации (ПА)	10	10
Всего:	42	42

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)
	<a href="https://lib.guap.ru/jirbis2/components/com_irbis/pdf_view/?869996">https://lib.guap.ru/jirbis2/components/com_irbis/pdf_view/?869996</a> Основы управления информационной безопасностью : учебное пособие / Н. Н. Мошак ; ред. В. В. Овчинников ; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - Санкт-Петербург : Изд-во ГУАП, 2022. - 141 с.	
	<a href="https://lib.guap.ru/jirbis2/components/com_irbis/pdf_view/?164521">https://lib.guap.ru/jirbis2/components/com_irbis/pdf_view/?164521</a> Безопасность информационных систем : [ Электронный ресурс] : учебное пособие / Н. Н. Мошак ; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - Санкт-Петербург : Изд-во ГУАП, 2019. - 169 с.	
	<a href="https://lib.guap.ru/jirbis2/components/com_irbis/pdf_view/?268708">https://lib.guap.ru/jirbis2/components/com_irbis/pdf_view/?268708</a> Организация безопасного доступа к информационным ресурсам : [ Электронный ресурс] : учебное пособие / Н. Н. Мошак, Т. М. Татарникова ; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - СПб. : Изд-во ГУАП, 2014. - 121 с.	
	<a href="https://lib.guap.ru/jirbis2/components/com_irbis/pdf_view/?850495">https://lib.guap.ru/jirbis2/components/com_irbis/pdf_view/?850495</a> 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.	
	<a href="http://znanium.com/catalog.php?bookinfo=402686">http://znanium.com/catalog.php?bookinfo=402686</a> Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.	
	<a href="https://e.lanbook.com/book/4925#book_name">https://e.lanbook.com/book/4925#book_name</a> Пушкарев, В.В. Защита информационных процессов в компьютерных системах. [Электронный ресурс] / В.В.	



Пушкарёв, В.П. Пушкарёв. — Электрон. дан. — М.: ТУСУР, 2012. — 131 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
1	ViPNet CSP
2	VirtualBox
3	OpenSSL
4	Монитор Zabbix
5	Учебно-методический комплекс ViPNet "Межсетевые экраны"
6	Учебно-методический комплекс ViPNet "Защита от несанкционированного доступа"
7	Программно-аппаратный комплекс ViPNet IDS (Практикум)

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	Фонд аудиторий ГУАП для проведения занятий лекционного и семинарского (практического) типа, групповых и индивидуальных консультаций, текущего	

	контроля и промежуточной аттестации. Специализированная мебель; технические средства обучения, служащие для представления учебной информации большой аудитории; переносной набор демонстрационного оборудования	
2	<b>Лаборатория программно-аппаратных средств обеспечения информационной безопасности</b> 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)	

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

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.
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения;

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
	<ul style="list-style-type: none"> <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.	Характеристика и состав процесса хранения данных	ПК-2.3.3
2.	Архитектуры хранения данных.	
3.	Физические компоненты систем хранения данных.	
4.	Интеллектуальные системы хранения данных.	
5.	Сети хранения данных	
6.	Цель резервного копирования.	
7.	Восстановление после отказа.	ПК-4.У.1
8.	Операционное резервное копирование.	ПК-4.В.1
9.	Архивирование.	ПК-6.В.1
10.	Локальная репликация.	ПК-1.3.6 ПК-2.3.2 ПК-2.3.3 ПК-2.3.4 ПК-2.У.1 ПК-4.3.2 ПК-4.3.3 ПК-4.У.1 ПК-4.У.2 ПК-4.У.3 ПК-4.В.1 ПК-6.У.1 ПК-6.В.1
11.	Технологии локальной репликации.	
12.	Удаленная репликация. Режимы удаленной репликации.	
13.	Технологии удаленной репликации: на основе хоста, на основе массива хранения данных, на основе SAN.	
14.	Триада риска: активы, угрозы, уязвимости.	
15.	Домены безопасности хранения.	
16.	Архитектура безопасности SAN.	
17.	Основные механизмы безопасности SAN.	
18.	Параметры для мониторинга инфраструктуры хранения.	
19.	Методы разграничения доступа к данным.	
20.	Особенности резервного копирования. Журналирование изменений.	
21.	Механизмы повышения защищённости, реализуемые в процессоре.	
22.	Механизмы повышения защищённости, реализуемые во внешних устройствах.	
23.	Механизмы защиты файловых систем.	
24.	Схема процесса обработки данных, угрозы и уязвимости	

	процесса.	
25.	Базовые технологии обеспечения безопасности процесса обработки данных.	
26.	Архитектура процесса передачи данных. Угрозы и уязвимости процесса.	
27.	Типичные проблемы безопасности в глобальных сетях	
28.	Типичные проблемы безопасности локальных сетей предприятий.	
29.	Средства защиты информации в открытых сетях.	ПК-2.3.2
30.	Защита данных на канальном уровне.	ПК-2.3.4
31.	Защита данных на сетевом уровне.	ПК-2.3.4
32.	Техническая реализация VPN на базе межсетевых экранов	ПК-1.3.6
33.	Техническая реализация VPN на базе маршрутизаторов	ПК-2.3.2
34.	Техническая реализация VPN на базе программного обеспечения	ПК-2.3.3 ПК-2.3.4
35.	Техническая реализация VPN на базе сетевой ОС	ПК-2.У.1
36.	Техническая реализация VPN на базе специализированных аппаратных средств.	ПК-4.3.2 ПК-4.3.3
37.	Функции и назначение межсетевых экранов.	ПК-4.У.1
38.	Создание демилитаризованной зоны.	ПК-4.У.2
39.	Схемы подключения межсетевых экранов.	ПК-4.У.3
40.	Системы обнаружения атак. Назначение, основные виды, особенности использования.	ПК-4.В.1
41.	Кольцевая система защиты памяти процессов.	ПК-6.У.1
42.	Особенности совместного использования процессами общих объектов в памяти.	ПК-6.В.1

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
	Не предусмотрено	

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:

Раздел 1. Введение

Раздел 2. Анализ возможных угроз в компьютерных системах.

Раздел 3. Особенности защиты информационного процесса хранения данных

Раздел 4. Особенности защиты информационного процесса обработки данных

Раздел 5. Особенности защиты информационного процесса передачи данных

11.2. Методические указания для обучающихся по выполнению 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 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

Вариант задания по каждой лабораторной работе обучающийся получает в соответствии с номером в списке группы. В соответствии с заданием обучающийся должен подготовить необходимые данные, получить от преподавателя допуск к выполнению лабораторной работы, выполнить указанную последовательность действий, получить требуемые результаты, оформить и защитить отчет по лабораторной работе.

#### 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 лабораторным работам выполняется отчет. Титульный лист оформляется в соответствии с шаблоном (образцом), приведенным на сайте ГУАП (<https://new.guap.ru/>) в разделе «Нормативная документация» (<https://guap.ru/standart/doc>). Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями, приведенными на сайте ГУАП в разделе «Нормативная документация» (<https://guap.ru/standart/doc>).

#### Методические указания по прохождению лабораторных работ:

- 1) Учебно-методический комплекс ViPNet "Межсетевые экраны"
- 2) Учебно-методический комплекс ViPNet "Защита от несанкционированного доступа"
- 3) Программно-аппаратный комплекс ViPNet IDS (Практикум)

#### 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.

#### 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.

Результаты текущего контроля учитываются при проведении промежуточной аттестации в соответствии с требованиями СТО ГУАП. СМК 3.76 «Положение о текущем

контроле успеваемости и промежуточной аттестации студентов и аспирантов ГУАП, обучающихся по образовательным программам высшего образования».

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:

– 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».

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». Зачет проводится в устной форме. Зачет обучающихся проводится, как правило, в течение недели, предшествующей началу экзаменационной сессии, либо на последнем занятии в семестре по дисциплине (модулю). Если со стороны обучающегося во время зачета допущены нарушения учебной дисциплины (списывание, несанкционированное использование средств мобильной связи, аудио–плееров и других технических устройств), нарушения правил внутреннего распорядка ГУАП, предпринята попытка подлога документов, преподаватель вправе удалить обучающегося с зачета с занесением в ведомость оценки «не зачтено». По результатам зачета «зачтено» заносится преподавателем в ведомость и зачетную книжку. Отрицательная оценка («не зачтено») заносится только в ведомость. Неявка обучающегося на зачет отмечается в ведомости словами «не явился», либо «н/я». Директор института на основе ведомости выясняет причину отсутствия обучающегося на зачете и принимает решение о порядке последующей сдачи.

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