

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

«Теоретические основы компьютерной безопасности»  
(Наименование дисциплины)

Код направления подготовки/ специальности	10.04.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности	Интеллектуальные средства обеспечения безопасности объектов
Форма обучения	очная

Санкт-Петербург – 2023

Лист согласования рабочей программы дисциплины

Программу составил (а)

доц.,к.т.н.,доц.

(должность, уч. степень, звание)



25.05.23

(подпись, дата)

В.А. Мыльников

(инициалы, фамилия)

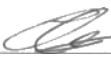
Программа одобрена на заседании кафедры № 33

«25» мая 2023 г, протокол № 10

Заведующий кафедрой № 33

д.т.н.,доц.

(уч. степень, звание)



25.05.23

(подпись, дата)

С.В. Беззатеев

(инициалы, фамилия)

Ответственный за ОП ВО 10.04.01(01)

доц.,к.т.н.,доц.

(должность, уч. степень, звание)



25.05.23

(подпись, дата)

В.А. Мыльников

(инициалы, фамилия)

Заместитель директора института №3 по методической работе



25.05.23

(подпись, дата)

Н.В. Решетникова

(инициалы, фамилия)

## Аннотация

Дисциплина «Теоретические основы компьютерной безопасности» входит в образовательную программу высшего образования – программу магистратуры по направлению подготовки/ специальности 10.04.01 «Информационная безопасность» направленности «Интеллектуальные средства обеспечения безопасности объектов». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-4 «Способен разрабатывать средства и системы защиты сетей электросвязи от несанкционированного доступа, а также защищённых телекоммуникационных систем»

ПК-7 «Способен проводить анализ угроз информационной безопасности в сетях электросвязи»

Содержание дисциплины охватывает круг вопросов, связанных с изучением теоретических вопросов компьютерной безопасности.

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 4 зачетных единицы, 144 часа.

Язык обучения по дисциплине «русский»

## 1. Перечень планируемых результатов обучения по дисциплине

### 1.1. Цели преподавания дисциплины

Цель преподавания дисциплины заключается в ознакомлении обучающихся с теоретическими вопросами компьютерной безопасности.

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-4 Способен разрабатывать средства и системы защиты сетей электросвязи от несанкционированного доступа, а также защищённых телекоммуникационных систем	ПК-4.З.1 знает методы, способы, средства, последовательность и содержание этапов разработки средств и систем защиты сетей от НСД, защищённых телекоммуникационных систем ПК-4.У.1 умеет разрабатывать проекты, технические задания, планы и графики проведения работ по защите сетей от НСД и необходимую техническую документацию ПК-4.В.1 владеет разработкой предложений и практической реализацией элементов, средств и систем защиты сетей от НСД, а также защищённых телекоммуникационных систем, включая разработку программного обеспечения
Профессиональные компетенции	ПК-7 Способен проводить анализ угроз информационной безопасности в сетях электросвязи	ПК-7.З.1 знает организационно-технические мероприятия по обеспечению защиты сетей электросвязи от НСД и их эффективность ПК-7.У.1 умеет проводить проверку работоспособности и эффективности применяемых программно-аппаратных (в том числе криптографических) и технических средств защиты сетей электросвязи от НСД ПК-7.В.1 владеет выработкой предложений по предотвращению и нейтрализации угроз НСД к сетям электросвязи

## 2. Место дисциплины в структуре ОП

Дисциплина может базироваться на знаниях, ранее приобретенных обучающимися при изучении соответствующих дисциплин программы бакалавриата.

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

- «Безопасность баз данных»,

- «Защищенные информационные системы»,
- «Технологии обеспечения информационной безопасности».

### 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
		№1
1	2	3
<b>Общая трудоемкость дисциплины, ЗЕ/ (час)</b>	4/ 144	4/ 144
<b>Из них часов практической подготовки</b>	51	51
<b>Аудиторные занятия, всего час.</b>	68	68
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)	17	17
экзамен, (час)	36	36
<b>Самостоятельная работа, всего (час)</b>	40	40
<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 1					
Раздел 1. Основные определения компьютерной безопасности.	2				12
Раздел 2. Задачи обеспечения компьютерной безопасности	8		16		12
Раздел 3. Сервисы безопасности на основе модели OSI (по ISO 7498-2).	7		16		12
Текущий контроль			2		4
Выполнение курсовой работы				17	
<b>Итого в семестре:</b>	17		34	17	40
<b>Итого</b>	17	0	34	17	40

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>	Раздел 1. Основные определения компьютерной безопасности. Тема 1.1. Объектно-ориентированный подход компьютерной безопасности. Суть объектно-ориентированного подхода. Комплексность решения. Создание рубежей защиты. Тема 1.2. Угрозы компьютерной безопасности конфиденциальности. Наиболее распространенные угрозы конфиденциальности, целостности, доступности. Тема 1.3. Модель нарушителя.
<b>2</b>	Раздел 2. Задачи обеспечения компьютерной безопасности. Тема 2.1. Управление доступом. Основы дискреционного управления доступом. Мандатное управление доступом. Тема 2.2. Методы аутентификации в компьютерных системах. Одно- и многофакторная аутентификация. Технологии решения. Тема 2.3. Методы обеспечения конфиденциальности. Модели шифрования. Основные типы криптоанализа.
<b>3</b>	Раздел 3. Сервисы безопасности на основе модели OSI (по ISO 7498-2). Тема 3.1. Протоколы, обеспечивающие решение задач информационной безопасности. Тема 3.2. Программно-аппаратные решения, обеспечивающие решение задач информационной безопасности. Тема 3.3. Системы обнаружения вторжений.

#### 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 1				
1	Реализация дискреционной модели доступа	8	8	2
2	Реализация мандатной модели доступа	8	8	2
3	Ознакомление с сетевыми сканерами	8	8	3
4	Ознакомление с брэндмауэрами	8	8	3
5	Текущий контроль	2	2	1-3
Всего		34	34	

#### 4.5. Курсовое проектирование/ выполнение курсовой работы

Цель курсовой работы:

Часов практической подготовки:

Примерные темы заданий на курсовую работу приведены в разделе 10 РПД.

#### 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 1, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	16	16
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	4	4
Домашнее задание (ДЗ)	20	20
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)		
Всего:	40	40

#### 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/M 87-604316-ED	Мошак Н. Н. Защищенные инфотелеком-муникации. Анализ и синтез [Электронный ресурс]: монография / Н. Н. Мошак; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - СПб.: Изд-во ГУАП, 2014. - 197 с.	50
004 Р 98	Рябко, Б. Я. Криптографические методы защиты информации [Текст]: учебное пособие / Б. Я. Рябко, А. Н. Фионов. - 2-е изд., стер. - М.: Горячая линия - Телеком, 2014. - 229 с.	10
004 М 48	Мельников, В. П. Защита информации [Текст]: учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе; ред. В. П. Мельников. - М.: Академия, 2014. - 304 с.	10
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
<a href="http://znanium.com/catalog.php?bookinfo=474838">http://znanium.com/catalog.php?bookinfo=474838</a>	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=423927">http://znanium.com/catalog.php?bookinfo=423927</a>	Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.	
<a href="http://znanium.com/catalog.php?bookinfo=471787">http://znanium.com/catalog.php?bookinfo=471787</a>	Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 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
<a href="http://www.iso27000.ru/chitalnyi-zai/upravlenie-informacionnoi-bezopasnostyu/praktika-upravleniya-informacionnoi-bezopasnostyu">http://www.iso27000.ru/chitalnyi-zai/upravlenie-informacionnoi-bezopasnostyu/praktika-upravleniya-informacionnoi-bezopasnostyu</a>	Практика управления информационной безопасностью
<a href="http://www.ict.edu.ru/catalog/index.php?a=nav&amp;c=getForm&amp;d=light&amp;id_res=1935&amp;r=navDesc">http://www.ict.edu.ru/catalog/index.php?a=nav&amp;c=getForm&amp;d=light&amp;id_res=1935&amp;r=navDesc</a>	Журнал "Защита информации. Конфидент"



## 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	Компьютерный класс	

## 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; Тесты.
Выполнение курсовой работы	Экспертная оценка на основе требований к содержанию курсовой работы по дисциплине.

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	

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>
«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
1	Объектно-ориентированный подход в информационной безопасности.	ПК-4.3.1
2	Угрозы конфиденциальности.	ПК-4.У.1
3	Угрозы целостности.	ПК-4.В.1
4	Угрозы доступности.	ПК-7.3.1
5	Модель нарушителя	ПК-7.У.1
6	Дискреционное управления доступом.	ПК-7.В.1
7	Базовая модель защиты ОС UNIX.	
8	Базовая модель защиты Windows.	
9	Основы X.500.	
10	Основы LDAP.	
11	Однофакторная аутентификация.	
12	Многофакторная аутентификация.	

13	Протоколы аутентификации.	
14	Мандатное управление доступом.	
15	Парольная аутентификация.	
16	Одноразовые пароли.	
17	Схема модификации одноразовых паролей.	
18	Система Kerberos.	
19	Биометрическая аутентификация.	
20	Основные типы криптоанализа.	
21	Принцип распределения ключей при традиционном шифровании.	
22	Хэширование сообщений.	
23	Принципы криптографии с открытым ключом.	
24	Основы цифровых подписи и сертификатов.	
25	Криптотуннели.	
26	Протокол IPsec.	
27	Межсетевые экраны.	
28	Схемы подключения межсетевых экранов.	
29	Архитектура протокола SSL.	
30	Принципы работы протокола PGP. Архитектура	
31	системы обнаружения вторжений.	
32	Системы обнаружения вторжений, основанные на статистических методах.	
33	Мониторинговые средства контроля компьютерной безопасности.	
34	Политика информационной безопасности и ее роль в обеспечении компьютерной безопасности	
35	Механизмы и технологии обеспечения безопасности хранения информации.	
36	Механизмы и технологии обеспечения безопасности передачи информации.	
37	Механизмы и технологии обеспечения безопасности обработки информации.	
38	Модель и жизненный цикл компьютерной атаки.	

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
1	Автоматизированная система обработки информации. Представление информации в АС Классификация возможных угроз информационной безопасности АС. Важные свойства информации и систем ее обработки.
2	Уровни доступа к информации. Анализ угроз информационной безопасности. Базовая эталонная модель взаимодействия открытых систем
3	Протокол. Сеть как набор протоколов

4	Стек протоколов TCP/IP. Соответствие уровней стека TCP/IP уровням модели OSI. IP адресация. Классы IP сетей. Характеристики классов IP-адресов. Выделенные IP-адреса.
5	Шлюзы и мосты. Маска подсети. Подсети - первый бастион защиты.
6	Интернет протоколы: Протокол пересылки файлов FTP; Протокол Telnet; Протокол SNMP; Протокол SMTP; Сетевая файловая система NFS; Протокол передачи гипертекста(HTTP); Сервис DNS.
7	Схема инкапсуляции данных в стеке протоколов TCP/IP. ARP-таблица.
8	Проблемы безопасности IP-сетей. Угрозы безопасности IP-сетей. Анализ угроз сетевой безопасности.
9	Схемы сетевой защиты на базе МЭ.
10	Формирование политики межсетевого взаимодействия. Основные схемы подключения МЭ.
11	Персональные и распределенные сетевые экраны.
12	Виртуальные защищенные сети (VPN).

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. Основные определения компьютерной безопасности.

Тема 1.1. Объектно-ориентированный подход компьютерной безопасности. Тема 1.2. Угрозы компьютерной безопасности

Тема 1.3. Модель нарушителя.

Раздел 2. Задачи обеспечения компьютерной безопасности. Тема 2.1. Управление доступом.

Тема 2.2. Методы аутентификации в компьютерных системах. Тема 2.3. Методы обеспечения конфиденциальности.

Раздел 3. Сервисы безопасности на основе модели OSI (по ISO 7498-2).

Тема 3.1. Протоколы, обеспечивающие решение задач информационной безопасности.

Тема 3.2. Программно-аппаратные решения, обеспечивающие решение задач информационной безопасности.

Тема 3.3. Системы обнаружения вторжений.

Структура предоставления материала каждой лекции состоит из:

- вступления (введения), где определяется тема, план и цель лекции. Обосновывается предмет лекции и ее актуальность, основная идея (проблема, центральный вопрос), связь с предыдущими и последующими занятиями, основные вопросы лекции.;
- изложения содержания, где реализуется научное содержание темы, все главные вопросы, приводится система доказательств с использованием наиболее целесообразных методических приемов. В ходе изложения применяются все формы и способы суждения, аргументации и доказательства. Все доказательства и разъяснения направлены на достижение поставленной цели, раскрытие основной идеи, содержания и научных выводов. Каждый учебный вопрос заканчивается краткими выводами, логически подводящими студентов к следующему вопросу лекции. Количество вопросов в лекции, как правило, от двух до четырех;
- заключения, где обобщаются в кратких формулировках основные идеи лекции, логически завершая ее как целостное изучение темы. В нем могут даваться рекомендации о порядке дальнейшего изучения основных вопросов лекции самостоятельно по указанной литературе.

## 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. Перед проведением лабораторной работы обучающемуся следует внимательно ознакомиться с методическими указаниями по ее выполнению. 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 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:

1. Шифр [004.056(075) Т 33] Теория информационной безопасности и методология защиты информации: методические указания к выполнению лабораторных работ № 1 - 4/ С. В. Беззатеев, Е. М. Линский, А. Д. Фомин. С.-Петербург. гос. ун-т аэрокосм. приборостроения; сост. - СПб.: ГОУ ВПО "СПбГУАП", 2007. - 35 с. Кол-во экз. в библиот. - 88.

2. Шифр [519.7 М 34] И. Л. Ерош, М. Ю. Литвинов, Н. В. Соловьев. Математические основы защиты информации: методические указания к выполнению лабораторных работ. СПб.: ГОУ ВПО "СПбГУАП", 2008. - 31 с.. Кол-во экз. в библиот. – 74.

*11.3. Методические указания для обучающихся по прохождению курсового проектирования/выполнения курсовой работы*  
Курсовой проект/ работа проводится с целью формирования у обучающихся опыта комплексного решения конкретных задач профессиональной деятельности.

Курсовой проект/ работа позволяет обучающемуся:

- систематизировать и закрепить полученные теоретические знания и практические умения по профессиональным учебным дисциплинам и модулям в

соответствии с требованиями к уровню подготовки, установленными программой учебной дисциплины, программой подготовки специалиста соответствующего уровня, квалификации;

- применить полученные знания, умения и практический опыт при решении комплексных задач, в соответствии с основными видами профессиональной деятельности по направлению/ специальности/ программе;
- углубить теоретические знания в соответствии с заданной темой;
- сформировать умения применять теоретические знания при решении нестандартных задач;
- приобрести опыт аналитической, расчётной, конструкторской работы и сформировать соответствующие умения;
- сформировать умения работы со специальной литературой, справочной, нормативной и правовой документацией и иными информационными источниками;
- сформировать умения формулировать логически обоснованные выводы, предложения и рекомендации по результатам выполнения работы;
- развить профессиональную письменную и устную речь обучающегося;
- развить системное мышление, творческую инициативу, самостоятельность, организованность и ответственность за принимаемые решения;
- сформировать навыки планомерной регулярной работы над решением поставленных задач.

#### Структура пояснительной записки курсового проекта/ работы

Текстовый документ должен включать в указанной ниже последовательности:

1. задание на курсовую работу;
2. содержание;
3. введение, в котором раскрываются актуальность и значение темы, выполняется краткий аналитический обзор, формулируется цель;
4. основную часть, структура и содержание которой зависит от характера работы;
5. заключение, в котором содержатся выводы и рекомендации относительно возможностей использования материалов работы;
6. список использованных источников;
7. приложения, содержащие материалы иллюстративного и вспомогательного характера;

Основная часть пояснительной записки курсового проекта, связанного с разработкой программного обеспечения, включает в себя:

- теоретические основы разрабатываемой темы;
- анализ задачи;
- обоснование выбора алгоритма для решения поставленной задачи из известных алгоритмов или создание оригинального алгоритма с описанием его правильности;
- подробное описание алгоритма;
- обоснование выбора языка программирования (если он не задан);
- обоснования выбора структур данных для представления исходных данных, результатов и промежуточных вычислений;
- руководство для пользователя, в котором описывается, как применять созданную программу;
- описание тестирования программы;
- результаты применения программы для решения поставленной задачи;
- листинги разработанных программ, помещаемые обычно в приложения

#### Требования к оформлению пояснительной записки курсового проекта/ работы

При оформлении пояснительной записки к курсовой работе следует пользоваться ГОСТ 7.32-2001. Правила оформления текстовых документов по ГОСТ 7.32-2001, а также титульные листы курсовых работ представлены на сайте ГУАП ([www.guar.ru](http://www.guar.ru)) в разделе «Сектор нормативной документации».

#### 11.4. 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 является учебно-методический материал по дисциплине.

Для развития у студентов навыков самостоятельного овладения теоретическим материалом ряд тем дисциплины на лекционных занятиях дается обзорно, что предполагает их самостоятельное детальное изучение.

Перечень тем для самостоятельного изучения:

- Объектно-ориентированный подход компьютерной безопасности.
- Модель нарушителя.
- Протоколы, обеспечивающие решение задач информационной безопасности.
- Программно-аппаратные решения, обеспечивающие решение задач информационной безопасности.
- Системы обнаружения вторжений.

#### 11.5. 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. Форма проведения текущего контроля – защита отчетов по лабораторным работам.

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».

#### 11.6. 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.

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».



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