

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. Мичурин

(инициалы, фамилия)



(подпись)

«25» мая 2023 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита сетей от несанкционированного доступа»
(Наименование дисциплины)

Код направления подготовки/ специальности	09.04.02
Наименование направления подготовки/ специальности	Информационные системы и технологии
Наименование направленности	Мультимедиа технологии
Форма обучения	очная

Санкт-Петербург– 2023

Лист согласования рабочей программы дисциплины

Программу составил (а)

Д.Т.Н., доц.
(должность, уч. степень, звание)

 25.05.23
(подпись, дата)

С.В. Беззатеев
(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 09.04.02(01)


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

 25.05.23
(подпись, дата)

О.И. Красильникова
(инициалы, фамилия)

Заместитель директора института №4 по методической работе

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

 25.05.23
(подпись, дата)

А.А. Ключарев
(инициалы, фамилия)

Аннотация

Дисциплина «Защита сетей от несанкционированного доступа» входит в образовательную программу высшего образования – программу магистратуры по направлению подготовки/ специальности 09.04.02 «Информационные системы и технологии» направленности «Мультимедиа технологии». Дисциплина реализуется кафедрой «№33».

Дисциплина не является обязательной при освоении обучающимся образовательной программы и направлена на углубленное формирование следующих компетенций:

ПК-4 «Способен определять структуру сети, устанавливать и руководить установкой сетевого программного обеспечения, обеспечивать бесперебойную работу сетей и инфокоммуникаций»

Содержание дисциплины охватывает круг вопросов, связанных с изучением теоретических и практических основ обеспечения информационной безопасности в пакетных мультисервисных сетях на технологии IP-QoS.

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

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

Общая трудоемкость освоения дисциплины составляет 1 зачетную единицу, 36 часов.

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью курса "Защита сетей от несанкционированного доступа" является изучение теоретических и практических основ обеспечения информационной безопасности в пакетных мультисервисных сетях на технологии IP-QoS.

1.2. Дисциплина является факультативной дисциплиной по направлению 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 определять структуру сети, устанавливать и руководить установкой сетевого программного обеспечения, обеспечивать бесперебойную работу сетей и инфокоммуникаций	ПК-4.3.1 знать принципы функционирования информационно-коммуникационных систем; типовые компоненты информационно-коммуникационной системы; основные технические характеристики, преимущества и недостатки продукции мировых и российских производителей информационно-коммуникационных систем и/или их составляющих; методики обеспечения высокой надежности и доступности; вопросы безопасности, решаемые на уровне дизайна информационно-коммуникационной системы

2. Место дисциплины в структуре ОП

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

- «Защита информационных процессов в компьютерных системах»,
- «Безопасность информационных систем».

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

- «Производственная 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
		№3
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	1/ 36	1/ 36
Из них часов практической подготовки		
Аудиторные занятия, всего час.	17	17
в том числе:		

лекции (Л), (час)	17	17
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)		
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		
Самостоятельная работа , всего (час)	19	19
Вид промежуточной аттестации: 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 3					
Раздел 1. Построение политики информационной безопасности пакетной мультисервисной сети	5				7
Раздел 2. Требования информационной безопасности пакетной мультисервисной сети	5				7
Раздел 3. Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	7				5
Итого в семестре:	17				19
Итого	17	0	0	0	19

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
1	Тема 1.1. Мультисервисные сети на технологиях IP-QoS и их основные функциональные элементы. Определение основных приоритетов информационной безопасности. Тема 1.2. Модели нарушителя и угроз.
2	Тема 2.1. Общие требования построения защищенной пакетной мультисервисной сети. Требования к подсистеме обеспечения безопасности сетевого взаимодействия. Тема 2.2. Требования к подсистеме аутентификации и управления доступом. Тема 2.3. Требования к подсистемам криптографической защиты информации и антивирусной защиты.

	<p>Тема 2.4. Требования к подсистемам резервирования/восстановления информации, контроля эталонного состояния информации и рабочей среды, управления безопасностью.</p> <p>Тема 2.5. Требования к средствам построения защищенных виртуальных сетей (VPN). Протокол формирования защищенного туннеля на канальном уровне PPTP (Point-to-Point Tunneling Protocol). Протокол формирования защищенного туннеля на канальном уровне L2F (Layer-2 Forwarding). Протокол формирования защищенного туннеля на канальном уровне L2TP (Layer-2 Tunneling Protocol). Общее описание стека протоколов защиты межсетевого уровня IPsec (Internet Protocol Security). Протокол обмена ключевой информацией IKE (Internet Key Exchange). Протокол аутентифицирующего заголовка (Authentication Header, AH). Протокол инкапсулирующей защиты содержимого (Encapsulating Security Payload, ESP).</p>
3	<p>Тема 3.1. Технические решения по защите от НСД межсетевого взаимодействия и передачи информации.</p> <p>Тема 3.2. Технические решения по защите от НСД компьютерных ресурсов на уровне серверов и рабочих станций ЛВС и реализации подсистемы аутентификации и идентификации</p>

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

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

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено				
Всего				

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 3, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	5	5
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	5	5
Домашнее задание (ДЗ)	5	5
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	4	4
Всего:	19	19

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	Мошак Н. Н. Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие / Н. Н. Мошак, Т. М. Татарникова. приборостроения. - СПб.: Изд-во ГУАП, 2014. - 121 с.	40
519.6./8 Т 98	Тюрликов А. М. Методы случайного множественного доступа [Текст]: монография /А. М. Тюрликов; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2014. - 300 с.	30
Ч404.3 М 48	Информационная безопасность и защита информации: учебное пособие/ В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред. С. А Клейменов. - 5-е изд.,	25

	стер. - М.: Академия, 2011. - 331 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
http://www.pgpru.com/	Проект "OpenPGP в России"

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	MS Windows
2	Учебно-методический комплекс ViPNet «Защита от несанкционированного доступа»
3	Учебно-методический комплекс ViPNet «Межсетевые экраны»
4	Блокхост-МДЗ, Блокхост-ЭЦП

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	Фонд лекционных аудиторий ГУАП	
2	Вычислительная лаборатория с компьютерами под управлением ОС Windows версии не ранее 7, объединенных в локальную сеть	

10. Оценочные средства для проведения промежуточной аттестации

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

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

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

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

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	<ul style="list-style-type: none"> – 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»	<ul style="list-style-type: none"> – 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»	<ul style="list-style-type: none"> – 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; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> – обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений.

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	Функционально-структурная организация	ПК-4.3.1
2	мультисервисной сети на технологии IntServ и DiffServ	
3	Сервисы безопасности и их реализация	
4	Определение основных приоритетов информационной безопасности в мультисервисной сети	
5	Модели нарушителя в мультисервисной сети	
6	Значимые угрозы в мультисервисной сети	
7	Общие требования построения защищенной мультисервисной сети	
8	Общие требования к подсистеме обеспечения безопасности сетевого взаимодействия	
9	Требования к подсистеме аутентификации и управления доступом	
10	Требования к подсистеме криптографической защиты информации	
11	Требования к подсистеме антивирусной защиты	
12	Требования к подсистеме резервирования и восстановления информации	
13	Требования к подсистеме контроля эталонного состояния информации и рабочей среды	
14	Требования к подсистеме управления безопасностью	
15	Требования к средствам построения защищенных виртуальных сетей (VPN)	
16	Технические решения по защите от НСД межсетевого взаимодействия и передаваемой информации	
17	Протокол формирования защищенного туннеля на канальном уровне L2F (Layer-2 Forwarding)	
18	Протокол формирования защищенного туннеля на канальном уровне L2TP (Layer-2 Tunneling Protocol)	
19	Общее описание стека протоколов защиты межсетевого уровня IPsec (Internet Protocol Security).	
20	Протокол обмена ключевой информацией IKE (Internet Key Exchange)	
21	Протокол аутентифицирующего заголовка (Authentication Header, AH);	
22	Протокол инкапсулирующей защиты содержимого (Encapsulating Security Payload, ESP).	
	Технические решения по защите от НСД компьютерных ресурсов на уровне серверов и рабочих станций ЛВС	
	Технические решения по реализации подсистемы аутентификации и идентификации	

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. Построение политики информационной безопасности пакетной мультисервисной сети.

Тема 1.1. Мультисервисные сети на технологиях IP-QoS и их основные функциональные элементы. Определение основных приоритетов информационной безопасности.

Тема 1.2. Модели нарушителя и угроз.

Раздел 2. Требования информационной безопасности пакетной мультисервисной сети.

Тема 2.1. Общие требования построения защищенной пакетной мультисервисной сети. Требования к подсистеме обеспечения безопасности сетевого взаимодействия. Тема 2.2.

Требования к подсистеме аутентификации и управления доступом.

Тема 2.3. Требования к подсистемам криптографической защиты информации и антивирусной защиты.

Тема 2.4. Требования к подсистемам резервирования/восстановления информации, контроля эталонного состояния информации и рабочей среды, управления безопасностью. Тема 2.5. Требования к средствам построения защищенных виртуальных сетей (VPN).

Раздел 3. Организационно-технические меры по реализации основных требований и построению системы информационной безопасности.

Тема 3.1. Технические решения по защите от НСД межсетевого взаимодействия и передачи информации.

Тема 3.2. Технические решения по защите от НСД компьютерных ресурсов на уровне серверов и рабочих станций ЛВС и реализации подсистемы аутентификации и идентификации.

11.2. 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;

11.3. 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.

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».

11.4. 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.

Зачет – 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».

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