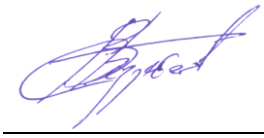
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 33

УТВЕРЖДАЮ
Руководитель направления

проф.,д.т.н.,доц.
(должность, уч. степень, звание)

С.В. Беззатеев
(инициалы, фамилия)



(подпись)
«27» мая 2022 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защищенные информационные системы»
(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– 2022

Лист согласования рабочей программы дисциплины

Программу составил (а)

доц.,к.т.н.,доц.	27.05.22	В.А. Мыльников
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«27» мая 2022 г, протокол № 10

Заведующий кафедрой № 33

д.т.н.,доц.	27.05.22	С.В. Беззатеев
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Ответственный за ОП ВО 10.04.01(01)

доц.,к.т.н.,доц.	27.05.22	В.А. Мыльников
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №3 по методической работе

	27.05.22	Н.В. Решетникова
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Аннотация

Дисциплина «Защищенные информационные системы» 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:

ОПК-1 «Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание»

ОПК-2 «Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности»

ОПК-4 «Способен осуществлять сбор, обработку и анализ научно- технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок»

ОПК-5 «Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно- технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи»

Содержание дисциплины охватывает круг вопросов, связанных с изучением терминологии, понятийного аппарата и общих подходов к обеспечению информационной безопасности автоматизированных систем.

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

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

Целью преподавания дисциплины «Анализ защищенности компьютерных систем» является изучение терминологии, понятийного аппарата и общих подходов к обеспечению информационной безопасности автоматизированных систем.

1.2. Дисциплина входит в состав обязательной части 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
Общепрофессиональные компетенции	ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.З.2 знать направления развития и проблемы компьютерного моделирования сложных систем; направления развития технологий проектирования информационных, автоматизированных и автоматических систем ОПК-1.З.3 знать современную нормативную базу и ГОСТы, регламентирующие процесс разработки ТЗ. Правила, способы и методы организации совместных разработок. ОПК-1.З.4 знать методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности ОПК-1.У.2 уметь обосновывать и планировать состав и архитектуру моделируемых сложных систем; обосновывать и планировать состав и архитектуру проектируемых информационных, автоматизированных и автоматических систем ОПК-1.У.3 уметь формировать актуальную модель угроз для АИС и учитывать её положения при формировании требований ТЗ на проектируемую систему обеспечения ИБ ОПК-1.У.4 уметь разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения ИБ. Оценивать эффективность решений и анализировать показатели деятельно-сти ОПК-1.У.5 уметь обосновывать принципы организации технического,

		программного и информационного обеспечения информационной безопасности ОПК-1.В.2 владеть навыками разработки концептуальных стратегий решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения ИБ ОПК-1.В.3 владеть навыками планирования и оценки трудоёмкости проекта, включая техническое, кадровое и финансовое обеспечение, принятие совместных решений
Общепрофессиональные компетенции	ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2.З.2 знать направления развития и проблемы компьютерного моделирования сложных систем; направления развития технологий проектирования информационных, автоматизированных и автоматических систем ОПК-2.З.3 знать современные методы и средства тестирования ОПК-2.З.4 знать принципы построения и функционирования современных информационных систем ОПК-2.У.2 уметь разрабатывать тестовые планы и сценарии тестирования разработанного продукта ОПК-2.У.3 уметь управлять коллективом исполнителей и принимать управленческие решения ОПК-2.В.2 владеть навыками практической реализации типовых задач разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью ОПК-2.В.3 владеть средствами автоматизированного и ручного функционального тестирования
Общепрофессиональные компетенции	ОПК-4 Способен осуществлять сбор, обработку и анализ научно- технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и	ОПК-4.У.3 уметь определять комплекс мер для обеспечения безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности систем ОПК-4.У.4 уметь использовать методы и средства анализа защищенности информационных систем
	технических разработок	
	ОПК-5 Способен	

Общепрофессиональные компетенции	проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	ОПК-5.З.9 знать принципы построения и функционирования современных информационных систем ОПК-5.В.4 владеет навыками выбора и обоснования критериев оценки защищенности открытых информационных систем

2. Место дисциплины в структуре ОП

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

– «Теоретические основы компьютерной безопасности»,

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и могут использоваться при написании выпускной квалификационной работы магистра

3. Объем и трудоемкость дисциплины

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

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№2
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	4/ 144	4/ 144
Из них часов практической подготовки		
Аудиторные занятия, всего час.	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
Самостоятельная работа, всего (час)	40	40
***Вид промежуточной аттестации*:** 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 2					
Раздел 1.Управление рисками.	5		4		7
Раздел 2. Методики построения системзащиты информации.	4		4		7
Раздел 3. Методики и программныепродукты для оценки рисков.	4		4		7
Раздел 4. Разработка рекомендаций поснижению рисков нарушения безопасности защищенной информационной системы.	4		5		7
Выполнение курсового проекта				17	12
Итого в семестре:	17		34	17	40
Итого	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
1	Тема 1.1. Модель безопасности с полным перекрытием. Тема 1.2. Стандарты в области информационной безопасности, использующие концепцию управление рисками ISO/IEC 15408. Тема 1.3. Критерии оценки безопасности информационных технологий. Тема 1.4. Стандарты ISO/IEC 17799/27002 и 27001
2	Тема 2.1. Модель многоуровневой защиты. Тема 2.2. Анализ существующих подходов построения систем защитыинформации. Тема 2.3. Технические мероприятия по снижению уровня риска.
3	Тема 3.1. Методика CRAMM. Тема 3.2. Методика FRAP. Тема 3.3. Методика OCTAVE. Тема 3.4. Методика RiskWatch.
4	Тема 4.1. Идентификация и аутентификация. Тема 4.2. Протокол Kerberos. Тема 4.3. Инфраструктура открытых ключей. Цифровые сертификаты.
	Тема 4.4. Протокол защиты электронной почты S/MIME. Тема 4.5. Протокол IPSec.

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 2				
1	Методики построения систем защиты информацииLifecycle Security	2		1
2	Методика управления рисками, предлагаемая Microsoft	2		2
3	Критерии оценки безопасности информационныхтехнологий.	2		1
4	Исследование методики CRAMM построения системзащиты информации	2		2, 3
5	Исследование методики OCTAVE построения системзащиты информации	2		2, 3
6	Исследование методики RiskWatch построения системзащиты информации	2		2, 3
7	Разработка модели многоуровневой защиты	2		2
8	Разработка рекомендаций по снижению рисков нарушениябезопасности защищенной информационной системы	2		2
9	Инфраструктура открытых ключей. Цифровые сертификаты.	1		4
	Всего	34	0	

4.5. Курсовое проектирование/ выполнение курсовой работы

Цель курсового проекта:

Примерные темы заданий на курсовой проект 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 2, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	10	10
Курсовое проектирование (КП, КР)	12	12
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	10	10
Домашнее задание (ДЗ)	8	8
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 Б 91	Бураков, М. В. Базы данных и язык SQL [Текст]: учебное пособие / М. В. Бураков, Р. Р. Латыпова; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2014. - 120 с.	50
004.4 М 15	Маклафлин, Б. PHP и MySQL. Исчерпываю-щее руководство [Текст] = PHP & MySQL. The missing manual / Б. Маклафлин. - 2-е изд. - СПб.: ПИТЕР, 2014. - 544 с.	30
004 М 87	Мошак Н. Н. Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие / Н. Н. Мошак, Т. М. Татарникова. - СПб.: Изд- во ГУАП, 2014. - 121 с.	40
004 К 56	Коваленко, В. В. Проектирование информационных систем [Текст]: учебное пособие / В. В. Коваленко. - М.: ФОРУМ: ИНФРА-М, 2015. - 320 с.	10
004.4 К 60	Колисниченко, Д. Н. PHP и MySQL. Разработка веб-приложений [Текст] /	5
	Д. Н. Колисниченко. -5-е изд. - СПб. : БХВ - Петербург, 2015. - 592 с.	
004 К 56	Коваленко, В. В. Проектирование информа- ционных систем: учебное пособие / В. В. Коваленко. - М.: ФОРУМ: ИНФРА-М, 2015. -320 с.	10
http://znanium.com/catalog.php?bookinfo=405313	Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 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://e.lanbook.com/view/book/1121/	Безопасность Oracle глазами аудитора: нападение и защита/А.М. Поляков ДМК Пресс, 2010, 336 с.

http://e.lanbook.com/view/book/1122/	Защита компьютерной информации/В.Ф. Шаньгин. - ДМК Пресс, 2010. 544 с.
http://www.znanium.com/bookread.php?book=175658	Комплексная система защиты информации на предприятии: учебное пособие/Н.В. Гришина. - М.: Форум, 2009, 240 с.
http://e.lanbook.com/view/book/1919/	Обеспечение безопасности организаций и производственных объектов: Практическое пособие для руководителей и работников предприятий и организаций/Петров С.В. ЭНАС, 2007, 224 с.

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	Операционная система MS Windows
2	Пакет MS Office
3	VMware ESXi

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 частиматериально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Компьютерный класс	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средствдля 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.
Выполнение курсового проекта	Экспертная оценка на основе требований к содержанию курсового проекта.

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
Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
	направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	– 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
1	Модель безопасности с полным перекрытием. Модель нарушителя. Оценка информационных рисков. Обработка информационных рисков. Управление рисками. Табличные методы оценки рисков. Архитектура информационной системы	ОПК-1.3.2

2	Современные стандарты в области информационной безопасности,использующие концепцию управление рисками ISO/IEC 15408. Оценочные стандарты ИБ.Ценность ресурсов ИС.	ОПК-2.З.3
3	Критерии оценки безопасности информационных систем. Стандарты управления ИБ	ОПК-2.З.4
4	Модель многоуровневой защиты. Анализ существующих подходов построения систем защиты информации.	ОПК-2.У.2
5	Технические мероприятия по снижению уровня риска. Сравнительные характеристики методов анализа рисков.	ОПК-2.У.3
6	Методика CRAMM. Недостатки. Методика CRAMM. Стадии исследования. Методика FRAP. Этапы оценки рисков. Методика FRAP. Построение матрицы рисков. Методика OCTAVE. Фазы анализа рисков. Методика OCTAVE. Построение профиля угрозы. Методика RiskWatch. Критерии оценки. Методика RiskWatch. Характеристика программного продукта. Эффект от внедрения.	ОПК-4.У.3
7	Идентификация и аутентификация. Протокол Kerberos. Инфраструктура открытых ключей. Цифровые сертификаты.	ОПК-4.У.4
8	Защита электронной почты. Протокол S/MIME. Протокол IPSec. Организационные мероприятия по защите информации вИС	ОПК-5.З.9
9	В последовательности из 6 двоичных символов имеется 3 единицы. При передаче данной последовательности сохраняется 3 символа, остальные теряются. Какова вероятность того, что среди сохранившихся будет не более 2 –х единиц?	ОПК-1.В.2
10	По каналу связи с помехами передается одна из двух команд управления в виде 11111 и 00000, вероятности передачи этих команд соответственно равны 0,7 и 0,3. Вероятность правильного приема каждого из символов 0 и 1 равна 0,6. Символы искажаются помехами независимо друг от друга. На выходе канала имеем кодовую комбинацию 10110. Определить какая комбинация была передана.	ОПК-1.В.3
11	о двоичному каналу связи с помехами передаются цифры 1 и 0 с вероятностями p1=p2=0.5. Вероятность перехода единицы в единицу и нуля в нуль соответственно равны p(1/1)=p, p(0/0)=q. Определить закон распределения вероятностей случайной величины X – однозначного числа,	ОПК-2.В.2

	получаемого на приемной стороне.	
12	Производится прием символов 0 и 1 до первого появления символа 1. Вероятность появления 1 при приеме p=0,4. Принимается не более четырех символов. Вычислить M(X), D(X), ( ) величины числа принятых символов.	ОПК-2.В.3
13	В алфавите некоторого языка всего две буквы. Каждое слово этого языка состоит из m букв. Известно, что можно составить 2048 различных слов. Сколько букв в каждом слове?	ОПК-5.В.4
14	1. Методы извлечения признаков при лицевой биометрии 2. Методы извлечения признаков при биометрии на основе радужной оболочки глаза 3. Методы извлечения признаков при голосовой идентификации 4. Методы извлечения признаков в поведенческой биометрии (на примере анализа почерка) 5. Методы извлечения признаков в поведенческой биометрии (на примере анализа движений глаз) 6. Методы извлечения признаков отпечатков пальцев 7. Методы извлечения признаков рисунка кровеносных сосудов ладони 8. Открытые базы данных по лицевой биометрии 9. Открытые базы данных по голосовой биометрии 10. Открытые базы данных по поведенческой биомерии	ОПК-1.З.3
15	1. Общая структура биометрической системы 2. Основные задачи биометрии (идентификация, верификация) 3. Критерии биометрических параметров 4. Гибридные биометрические методы 5. Поведенческие биометрические параметры 6. Виды ошибок в биометрических системах. Кривые РХПУ 7. Качество работы биометрических систем. Понятие отрицательной аутентификации 8. Идентификация по порогу, идентификация при помощи ранжирования 9. Статистики ранговых отношений. Функция массы ранговой вероятности 10. Тестирование биометрической системы. Технологическая и сценарная оценки 11. Выбор биометрических параметров 12. Регистрация субъектов в биометрической системе. Модель зоопарка 13. Регистрация как обучение системы 14. Крупномасштабные приложения биометрических систем 15. Атаки на биометрическую систему. Основные виды 16. Атаки презентацией. Методы обнаружения спуфинга	ОПК-1.У.4
16	1. Методы регистрации основных биометрических параметров (лицо) 2. Методы регистрации основных биометрических параметров (радужная оболочка)	ОПК-1.У.5

	3. Методы регистрации основных биометрических параметров (голос) 4. Методы регистрации основных биометрических параметров (отпечатки пальцев) 5. Пример построения кривой РХПУ 6. Оценки КЛД(m) и КЛОД(m) в базовом («простом») приближении 7. Точные оценки КЛД(m) и КЛОД(m) 8. Оценка доверительных интервалов величин сходства. Описание метода бутстрапа 9. Доверительные интервалы в оценке КЛД и КЛОД 10. Методы интеграции биометрической информации. Булево комбинирование 11. Методы интеграции биометрической информации. Уровень распределений степеней принадлежности	
17	1. Опишите структуру современной системы электронных меж банковских расчетов в России. 2. Как вы понимаете такие характеристики электронных платежей, как гарантированность и безотзывность? 3. В чем отличие электронных платежных документов полного и сокращенного формата? 36 4. Что понимается под электронной цифровой подписью и при формировании каких документов она используется? 5. Определите, верно или нет утверждение: Банк России допускает внесение определенных изменений в электронные платежные документы, поступившие в расчетную сеть Банка России. 6. Перечислите документы, на основании которых производятся платежи в системе внутрирегиональных электронных расчетов. 7. Дайте ответ, верно ли утверждение: внутрирегиональные электронные платежи должны выполняться «день в день». 8. Назовите способы обработки учетно-операционной информа ции при межбанковских электронных расчетах. 9. Что такое «квитовка» электронных платежных документов и как она происходит? 10. Как осуществляется программный и логический контроль межрегиональных электронных платежей? Кто его проводит? 11. Как обеспечивается безопасность и защита информации в платежной системе Банка России?	ОПК-2.3.2
18	1. Формальные средства защиты. Аппаратные средства защиты. 2. Физические средства защиты. 3. Программные средства защиты. 4. Неформальные средства защиты.. 5. Организационные средства защиты.	ОПК-1.3.4

	6. Законодательные меры защиты. 7. Морально-этические нормы 8. Аппаратно-программные средства защиты информации в ПЭВМ. 9. Вирусы и антивирусы. 10. Обеспечение целостности информации, передаваемой в сетях ЭВМ	
19	1. В основу системы классификации АС должны быть положены следующие характеристики объектов и субъектов защиты, а также способов их взаимодействия: 1. информационные 2. организационные 3. технологические 4. правовые 5. системные 6. экономические 2. Какие степени секретности и грифы секретности носителей сведений, установлены законодательством РФ. Отметьте правильный вариант: 1. для служебного пользования 2. совершенно секретно 3. конфиденциально 4. особой важности 5. строго конфиденциально 6. секретно 3. Технологические характеристики АС используемые для классификации, включают в себя: 1. способ обработки 2. время циркуляции информации (транзит, хранение) 3. вид АС (автономная, сеть, стационарная, подвижная) 4. состав средств вычислительной техники, используемой в процессе обработки информации категория информации и ее объемы 4. Средства криптографической защиты информации (СКЗИ) это: совокупность территориально распределенной инфраструктуры программных и технических средств, Администраторов и Операторов Удостоверяющего центра, обеспечивающих деятельность по изготовлению и управлению сертификатами ключей проверки подписей пользователей Удостоверяющего центра и выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи» 1. уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи 2. аппаратные, программные или аппаратно-программные средства, осуществляющие криптографические преобразования информации для обеспечения ее безопасности 3. программные и (или) аппаратные средства, используемые для реализации функций	ОПК-1.У.2

	удостоверяющего центра 5. Защита АС должна обеспечиваться. Отметьте правильные варианты ответа: 1. на всех технологических этапах обработки информации 2. во всех режимах работы СВТ, в которых выполняется обработка защищаемой информации 3. при проведении ремонтных и регламентных работ 4. в местах хранениях информации на съемных машинных носителях 5. только при обработке информации СВТ АС 6. Инцидент информационной безопасности это: идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности 1. одно или серия нежелательных или неожиданных событий информационной безопасности, имеющих значительную вероятность нарушения бизнес операций или представляющих угрозу для информационной безопасности 2. процесс сравнения оценочной величины риска с установленным критерием с целью определения уровня значимости риска 3. слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами 7. Загрузочные (бутовые) вирусы это: 1. вирусы, заражающие программы, хранящиеся в системных областях дисков 2. вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам 3. вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса 4. ни один из ответов не является верным 8. Мероприятия по инженерно-технической защите информации от утечки по электромагнитному каналу подразделяются на: 1. организационные и технические 2. технические и коммутационные 3. организационные и объективные 4. ни один из ответов не является верным 9. Организационно-техническими методами обеспечения информационной безопасности являются. Отметьте правильные варианты ответов: 1. разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств 2. развитие защищенных телекоммуникационных систем	

	3. создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации 4. создание систем и средств предотвращения специальных воздействий, вызывающих разрушение, уничтожение, искажение информации 5. создание систем и средств предотвращения специальных воздействий, вызывающих изменение штатных режимов функционирования систем и средств информатизации и связи 6. сертификация средств защиты информации 27 7. контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности	
20	1. Дать определение и характеристику основных режимов работы, дисциплин и режимов обслуживания заявок в вычислительных системах. 2. Дать определение и характеристику классов программных средств. 3. Изложить классификацию ОС. 4. Охарактеризовать основные принципы построения ОС. 5. Перечислить виды интерфейсов ОС. Охарактеризовать пакетную технологию как интерфейс. Дать описание интерфейса командной строки. 6. Дать описание графических интерфейсов. В каких ОС они применяются? 7. Охарактеризовать речевую технологию как интерфейс. 8. Охарактеризовать биометрическую технологию как интерфейс. 9. Охарактеризовать семантический интерфейс. 10. Дать определение понятия процесса. Зачем оно требуется? 11. Дать определение понятия прерывания. Зачем оно требуется? 12. Дать определение понятия виртуальности. Зачем оно требуется? 13. Дать определение понятия ресурса. Зачем оно требуется? 14. Охарактеризуйте понятие "ядро ОС"? 15. Охарактеризуйте понятие "микроядро ОС"? 16. Описать организацию управления в ОС. 17. Перечислить дисциплины обслуживания. 18. Перечислить режимы обслуживания. 19. Описать средства управления задачами на уровне внешнего планирования. 20. Дать определение понятия "контекст процесса". 21. Пояснить понятия "нить" и "процесс". 22. Назвать состав алгоритмов внутреннего планирования. 23. Охарактеризовать алгоритмы управления количеством процессов в рабочей смеси. 24. Охарактеризовать алгоритмы выбора очередности	ОПК-1.У.3

	обработки. 25. Охарактеризовать алгоритмы выбора величины кванта 26. Дать определение понятий параллельных процессов, критического ресурса, критического участка. 27. Что такое "примитивы взаимоисключения"? 28. Каковы механизмы реализации примитивов взаимоисключения? 29. Описать алгоритмы предотвращения тупиков. 30. Описать алгоритмы обхода тупиков.	

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	Источники, риски и формы атак на компьютерные системы
2	Модели безопасности информационных систем
3	Защита информации в современных операционных системах
4	Защита информации в сети
5	Виды политик информационной безопасности
6	Математические модели информационной безопасности
7	Технологии аутентификации
8	Защита информации на прикладном уровне
9	Система отслеживания вторжений

Вопросы для проведения промежуточной аттестации в виде тестированияпредставлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора

	1) К правовым методам, обеспечивающим информационную безопасность, относятся: - Разработка аппаратных средств обеспечения правовых данных - Разработка и установка во всех компьютерных правовых сетях журналов учета действий + Разработка и конкретизация правовых нормативных актов обеспечения безопасности **2) Основными источниками угроз информационной безопасности являются все указанное в списке:** - Хищение жестких дисков, подключение к сети, инсайдерство + Перехват данных, хищение данных, изменение архитектуры системы - Хищение данных, подкуп системных администраторов, нарушение регламента работы **3) Виды информационной безопасности:** + Персональная, корпоративная, государственная - Клиентская, серверная, сетевая - Локальная, глобальная, смешанная	ОПК-1.У.4
	4) Цели информационной безопасности – своевременное обнаружение, предупреждение: + несанкционированного доступа, воздействия в сети - инсайдерства в организации - чрезвычайных ситуаций **5) Основные объекты информационной безопасности:** + Компьютерные сети, базы данных - Информационные системы, психологическое состояние пользователей - Бизнес-ориентированные, коммерческие системы **6) Основными рисками информационной безопасности являются:** - Искажение, уменьшение объема, перекодировка информации - Техническое вмешательство, выведение из строя оборудования сети + Потеря, искажение, утечка информации	ОПК-1.У.5

	7) К основным принципам обеспечения информационной безопасности относится: + Экономической эффективности системы безопасности - Многоплатформенной реализации системы - Усиления защищенности всех звеньев системы **8) Основными субъектами информационной безопасности являются:** - руководители, менеджеры, администраторы компаний + органы права, государства, бизнеса - сетевые базы данных, фаерволлы **9) К основным функциям системы безопасности можно отнести все перечисленное:** + Установление регламента, аудит системы, выявление рисков - Установка новых офисных приложений, смена хостинг-компании - Внедрение аутентификации, проверки контактных данных пользователей **12) Принципом политики информационной безопасности является принцип:** + Усиления защищенности самого незащищенного звена сети (системы) - Перехода в безопасное состояние работы сети, системы - Полного доступа пользователей ко всем ресурсам сети, системы **13) Принципом политики информационной безопасности является принцип:** + Разделения доступа (обязанностей, привилегий) клиентам сети (системы)	ОПК-1.У.2
	10) Принципом информационной безопасности является принцип недопущения: + Неоправданных ограничений при работе в сети (системе) - Рисков безопасности сети, системы - Презумпции секретности **11) Принципом политики информационной безопасности является принцип:** + Невозможности миновать защитные средства сети (системы) - Усиления основного звена сети, системы - Полного блокирования доступа при риск-ситуациях	ОПК-1.У.3

Перечень тем контрольных работ по дисциплине обучающихся заочной формыобучения, 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.Управление рисками.
Тема 1.1. Модель безопасности с полным перекрытием.
Тема 1.2. Стандарты в области информационной безопасности, использующие концепцию управление рисками ISO/IEC 15408.
Тема 1.3. Критерии оценки безопасности информационных технологий.Тема 1.4.
Стандарты ISO/IEC 17799/27002 и 27001.
Раздел 2. Методики построения систем защиты информации.Тема 2.1.
Модель многоуровневой защиты.
Тема 2.2. Анализ существующих подходов построения систем защиты информации.
Тема 2.3. Технические мероприятия по снижению уровня риска. Раздел 3.
Методики и программные продукты для оценки рисков.Тема 3.1. Методика
CRAMM.
Тема 3.2. Методика FRAP. Тема 3.3.
Методика OCTAVE. Тема 3.4. Методика
RiskWatch.
Раздел 4. Разработка рекомендаций по снижению рисков нарушения безопасности защищенной информационной системы.
Тема 4.1. Идентификация и аутентификация.Тема 4.2.
Протокол Kerberos.
Тема 4.3. Инфраструктура открытых ключей. Цифровые сертификаты.Тема 4.4.
Протокол защиты электронной почты S/MIME.
Тема 4.5. Протокол IPSec..

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) в разделе «Сектор нормативной документации». Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями, приведенными на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации».
Методические указания по прохождению лабораторных работ:

1. [004.056(075) Т 33] Беззатеев С. В. Теория информационной безопасности и методология защиты информации: методические указания к выполнению лабораторных работ № 1. - СПб.: ГОУ ВПО "СПбГУАП", 2007. Кол-во экз. в библ. – 88.
2. [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 библ. – 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

1. Постановка задачи
2. Основная часть
3. Расчетная/аналитическая часть
4. Выводы

Требования к оформлению пояснительной записки курсового проекта/ работы

– Оформление с использованием стилей
– MS Word (OO Writer) или TeX
– Наличие оглавления
– Наличие ссылок на литературу
– Наличие подписей к картинкам

Титульный лист оформляется в соответствии с шаблоном (образцом) приведенным на сайте ГУАП (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) 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:

- Модель безопасности с полным перекрытием.
- Стандарты в области информационной безопасности, использующие концепцию управление рисками ISO/IEC 15408.
- Критерии оценки безопасности информационных технологий.
- Стандарты ISO/IEC 17799/27002 и 27001.
- Технические мероприятия по снижению уровня риска.
- Методика CRAMM.
- Методика FRAP.
- Методика OCTAVE.
- Методика RiskWatch.
- Протокол защиты электронной почты S/MIME.

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.
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