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

Кафедра № 33

УТВЕРЖДАЮ
Ответственный за образовательную программу

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

С.В. Беззатеев
(инициалы, фамилия)

(подпись)

«27» июня 2024 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационная безопасность распределенных информационных систем»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.05.03
Наименование направления подготовки/ специальности	Информационная безопасность автоматизированных систем
Наименование направленности	Безопасность открытых информационных систем
Форма обучения	очная
Год приема	2024

Санкт-Петербург– 2024

Лист согласования рабочей программы дисциплины

Программу составил (а)

проф.,к.т.н.,проф. (должность, уч. степень, звание) | 27.06.2024 (подпись, дата) | С.Г. Фомичева (инициалы, фамилия)

Программа одобрена на заседании кафедры № 33
«27» июня 2024 г, протокол № 11

Заведующий кафедрой № 33

д.т.н.,доц. (уч. степень, звание) | 27.06.2024 (подпись, дата) | С.В. Беззатеев (инициалы, фамилия)

Заместитель директора института №3 по методической работе

(должность, уч. степень, звание) | 27.06.2024 (подпись, дата) | Н.В. Решетникова (инициалы, фамилия)

Аннотация

Дисциплина «Информационная безопасность распределенных информационных систем» входит в образовательную программу высшего образования – программу специалитета по направлению подготовки/ специальности 10.05.03 «Информационная безопасность автоматизированных систем» направленности «Безопасность открытых информационных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-1 «Способен выполнять работы по проектированию автоматизированных информационных систем»

ПК-2 «Способен формировать требования к защите информации в открытых информационных системах»

ПК-3 «Способен разрабатывать средства защиты сетей связи от несанкционированного доступа»

ПК-4 «Способен осуществлять работы по разработке систем защиты информации автоматизированных систем»

ПК-7 «Способен управлять развитием средств защиты открытых информационных систем от несанкционированного доступа»

ПК-9 «Способен осуществлять работы по оценке работоспособности и эффективности применяемых программно-аппаратных средств защиты информации»

ПК-10 «Способен осуществлять организацию работ по выполнению в автоматизированных системах требований защиты информации»

ПК-11 «Способен проводить оценку уровня информационной безопасности открытых информационных систем»

Содержание дисциплины охватывает круг вопросов, связанных с изучением архитектуры распределенных информационных систем (РИС), особенностей защиты информации в РИС, обеспечением безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС, защитой информации на уровне подсистемы управления, защитой информации в каналах связи и особенностями защиты информации в базах данных.

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

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 «Информационная безопасность распределенных информационных систем» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» заключается в приобретении теоретических знаний и формировании практических навыков, связанных с проектированием архитектуры распределенных ИС, разработкой системы защиты информации в РИС, обеспечением безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС, организации защиты информации на уровне подсистемы управления, в каналах связи и в распределенных базах данных.

1.2. Дисциплина входит в состав части, формируемой участниками образовательных отношений, образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Профессиональные компетенции	ПК-1 Способен выполнять работы по проектированию автоматизированных информационных систем	ПК-1.В.1 владеть навыками сбора сведений для информационно-коммуникационной системы и межсетевых соединений
Профессиональные компетенции	ПК-2 Способен формировать требования к защите информации в открытых информационных системах	ПК-2.З.2 знать программно-аппаратные средства обеспечения защиты информации автоматизированных систем ПК-2.З.7 знать методы защиты информации от "утечки" по техническим каналам ПК-2.У.4 уметь анализировать возможные уязвимости информационных систем ПК-2.У.5 уметь выявлять известные уязвимости информационных систем
Профессиональные компетенции	ПК-3 Способен разрабатывать средства защиты сетей связи от несанкционированного доступа	ПК-3.В.1 владеть навыками оценки уязвимости сетей
Профессиональные компетенции	ПК-4 Способен осуществлять работы по разработке систем защиты информации автоматизированных систем	ПК-4.З.2 знать особенности защиты информации в открытых информационных системах ПК-4.З.4 знать принципы формирования политики информационной безопасности в автоматизированных системах
Профессиональные компетенции	ПК-7 Способен управлять развитием средств защиты открытых	ПК-7.У.1 уметь проводить анализ угроз несанкционированного доступа

	информационных систем от несанкционированного доступа	
Профессиональные компетенции	ПК-9 Способен осуществлять работы по оценке работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	ПК-9.З.2 знать порядок организации работ по защите информации
Профессиональные компетенции	ПК-10 Способен осуществлять организацию работ по выполнению в автоматизированных системах требований защиты информации	ПК-10.З.2 знать защитные механизмы и средства обеспечения безопасности автоматизированных систем ПК-10.У.1 уметь определять методы управления доступом, типы доступа и правила разграничения доступа ПК-10.У.2 уметь классифицировать защищаемую информацию по видам тайны и степени конфиденциальности ПК-10.В.2 владеть навыками организации процесса разработки моделей угроз и моделей нарушителя безопасности компьютерных систем
Профессиональные компетенции	ПК-11 Способен проводить оценку уровня информационной безопасности открытых информационных систем	ПК-11.З.1 знать методы и методики оценки безопасности программно-аппаратных средств защиты информации ПК-11.З.2 знать принципы построения подсистем защиты информации ПК-11.У.1 уметь определять параметры функционирования средств защиты информации, разрабатывать методики оценки их защищенности, оценивать эффективность защиты информации

2. Место дисциплины в структуре ОП

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

- «Технологии и методы программирования»
- «Основы информационной безопасности»
- «Теория систем и системный анализ»
- «Безопасность сетей ЭВМ»
- «Защита информации от утечки по техническим каналам»
- «Методы и средства криптографической защиты информации»
- «Организация ЭВМ и вычислительных систем»
- «Сети и системы передачи информации»
- «Организационное и правовое обеспечение информационной безопасности»
- «Программно-аппаратные средства защиты информации»
- «Разработка и эксплуатация автоматизированных систем в защищенном исполнении»

– «Управление информационной безопасностью»
– «Методы и средства проектирования информационных систем»
– «Теория информационной безопасности»
– «Защита информации в распределенных информационных системах»

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

– « Производственная преддипломная практика»,
– «Государственная итоговая аттестация»

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
		№10
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	4/ 144	4/ 144
Из них часов практической подготовки	34	34
Аудиторные занятия, всего час.	68	68
в том числе:		
лекции (Л), (час)	34	34
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	34	34
курсовой проект (работа) (КП, КР), (час)		
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 10					
Раздел 1.Архитектура распределенных ИС Тема 1.1.Классификация РИС Тема 1.2.Коммутационная подсистема РИС: коммутационные модули (КМ); каналы связи; концентраторы; межсетевые шлюзы. Тема 1.3.Подсистемы РИС: пользовательская; подсистема управления; коммуникационная подсистема	4		4		6

Раздел 2. Особенности защиты информации в РИС Тема 2.1. Корпоративные и общедоступные РИС. Построение системы защиты информации в РИС. Тема 2.2. Особенности защиты информации от непреднамеренных угроз в РИС. Пассивные и активные угрозы безопасности информации в РИС. Тема 2.3. Меры, предпринимаемые для обеспечения безопасности информации в сосредоточенных ИС, механизмы для защиты информации при передаче ее по каналам связи Тема 2.4. Методы и средства, обеспечивающие безопасность информации в защищенной вычислительной сети	6		6		6
Раздел 3. Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС Тема 3.1. Поддержка механизмов аутентификации и разграничения доступа Тема 3.2. Специализированные коммуникационные компьютерные системы. Тема 3.3. Центр управления сетью. Средства защиты информации, специализированной ИС администратора сети	6		6		6
Раздел 4. Защита информации на уровне подсистемы управления Тема 4.1. Управление передачей сообщений по определенным протоколами. Тема 4.2. Международные стандарты взаимодействия удаленных элементов сети: протокол TCP/IP и протокол X.25.Модель OSI. Тема 4.3. Проблемы защиты информации в РИС	6		6		6
Раздел 5. Защита информации в каналах связи Тема 5.1 Комплекс методов и средств защиты, позволяющих блокировать возможные угрозы безопасности информации. Тема 5.2. Процедуры взаимного подтверждения подлинности абонентов или процессов. Тема 5.3. Использование криптографических методов защиты	6		6		6
Раздел 6. Особенности защиты информации в распределенных базах данных Тема 6.1 Реляционные и нереляционные базы данных. Функции управления данными, Тема 6.2. Особенности защиты информации в базах данных. Тема 6.3. Разграничение доступа к файлам баз данных и к частям баз данных Тема 6.4.Режимы работы с зашифрованными базами данных. Тема 6.5.Методы противодействия угрозам информации в базах данных	6		6		10
Итого в семестре:	34		34		40
Итого	34	0	34	0	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	**Архитектура распределенных ИС** Тема 1.1.Классификация РИС (демонстрация слайдов) Тема 1.2.Коммутационная подсистема РИС: коммутационные модули (КМ); каналы связи; межсетевые экраны (демонстрация слайдов) Тема 1.3.Подсистемы РИС: пользовательская; подсистема управления; коммуникационная подсистема (демонстрация слайдов)
2	**Особенности защиты информации в РИС** Тема 2.1. Построение частных моделей угроз. (демонстрация слайдов) Тема 2.2. Особенности защиты информации от непреднамеренных угроз в РИС. Пассивные и активные угрозы безопасности информации в РИС. (демонстрация слайдов) Тема 2.3. Меры, предпринимаемые для обеспечения безопасности информации в сосредоточенных ИС, механизмы для защиты информации при передаче ее по каналам связи (демонстрация слайдов) Тема 2.4. Методы и средства, обеспечивающие безопасность информации в защищенной вычислительной сети (демонстрация слайдов)
3	**Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС** Тема 3.1. Поддержка механизмов аутентификации и разграничения доступа (демонстрация слайдов) Тема 3.2. Специализированные коммуникационные компьютерные системы. (демонстрация слайдов) Тема 3.3. SIEM-решения - как средства защиты информации в РИС (демонстрация слайдов)
4	**Защита информации на уровне подсистемы управления** Тема 4.1. Управление передачей сообщений по определенным протоколами. (демонстрация слайдов) Тема 4.2. Международные стандарты взаимодействия удаленных элементов сети: протокол TCP/IP и протокол X.25.Модель OSI. (демонстрация слайдов) Тема 4.3. Проблемы защиты информации в РИС. (демонстрация слайдов)
5	**Защита информации в каналах связи.** Тема 5.1 Комплекс методов и средств защиты, позволяющих блокировать возможные угрозы безопасности информации. (демонстрация слайдов) Тема 5.2. Процедуры взаимного подтверждения подлинности абонентов или процессов. (демонстрация слайдов) Тема 5.3. Использование криптографических методов защиты (демонстрация слайдов)
6	**Особенности защиты информации в распределенных базах данных** Тема 6.1 Реляционные и нереляционные базы данных. Функции управления данными, (демонстрация слайдов) Тема 6.2. Особенности защиты информации в базах данных. (демонстрация слайдов) Тема 6.3. Разграничение доступа к базе данных и к частям баз данных (демонстрация слайдов) Тема 6.4.Режимы работы с зашифрованными базами данных. (демонстрация слайдов) Тема 6.5.Методы противодействия угрозам информации в базах данных

	(демонстрация слайдов)

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 10				
1	«Разработка модели угроз безопасности информации»	4	2	2
2	«Формирование структуры базы данных РИС»	6	4	1, 6
3	«Оценка и приоритизация рисков ИБ РРС»	6	4	3, 5
4	«Сбор логов событий информационной безопасности»	6	4	4, 5, 6
5	«Разработка Web-клиента мониторинга исключений в распределенной информационной системе»	6	4	1, 4, 5, 6
Всего		34		

4.5. Курсовое проектирование/ выполнение курсовой работы

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 10, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	20	20

Курсовое проектирование (КП, КР)	-	-
Расчетно-графические задания (РГЗ)	-	-
Выполнение реферата (Р)	-	-
Подготовка к текущему контролю успеваемости (ТКУ)	10	10
Домашнее задание (ДЗ)	-	-
Контрольные работы заочников (КРЗ)	-	-
Подготовка к промежуточной аттестации (ПА)	10	10
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 Ф 76	Фомичева, Светлана Григорьевна. Обработка информации в распределенных системах : учебное пособие / С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2020. - 132 с. ; 131 с. : рис. - Библиогр.: с. 123 (17 назв.). - ISBN 978-5-8088-1487-5 : Б. ц. - Текст : непосредственный	5
004 Б 39	Беззатеев, Сергей Валентинович (д-р техн. наук, доц.). Программирование задач по обеспечению информационной безопасности : лабораторный практикум / С. В. Беззатеев, С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2020. - 89 с. : рис., табл. - Библиогр.: с. 88 (10 назв.). - Б. ц. - Текст : непосредственный.	5
004 З-62	Зима, В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. - 2-е изд. - СПб. : БХВ - Петербург, 2015. - 368 с. : рис. - (Мастер систем). - Библиогр.: с. 351 - 353 (31 назв.).- Предм. указ.:с. 354 - 362. - ISBN 978-5-94157-213-7 : 419.00 р. - Текст : непосредственный	7

007 В 67	Волкова, В. Н. Теория систем и системный анализ : учебник для академического бакалавриата / В. Н. Волкова, А. А. Денисов ; Нац. исслед. С.-Петерб. гос. политехн. ун-т. - 2-е изд., перераб. и доп. - М. : Юрайт, 2015. - 616 с. : рис. - (Бакалавр. Академический курс). - Предм. указ.: с. 600 - 606. - Имен. указ.: с. 607 - 609. - Библиогр.: с. 610 - 616 (109 назв.). - ISBN 978-5-9916-4783-0 : 870.87 р. - Текст : непосредственный. Имеет гриф УМО высшего образования	10
004 И 85	Исаев, Г. Н. Проектирование информационных систем : учебное пособие / Г. Н. Исаев. - 2-е изд., стер. - М. : ОМЕГА-Л, 2015. - 424 с. : рис., табл. - (Высшее техническое образование). - Библиогр.: с. 421 - 424 (61 назв.) . - ISBN 978-5-370-03507-4 : 401.60 р. - Текст : непосредственный. На стр. 7 - 8: Список сокращений	5
004 Б 24	Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. - 3-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2017. - 322 с. : рис., табл. - (Высшее образование). - Библиогр.: с. 313 - 316 (56 назв.). - ISBN 978-5-369-01450-9 (РИОР). - ISBN 978-5-16-011164-3 (ИНФРА-М) : 942.63 р. - Текст : непосредственный. Имеет гриф УМО по образованию в области прикладной информатики	5
004.4 И 46	Ильина, Дарья Викторовна. Проектирование и разработка безопасных веб-приложений : учебное пособие / Д. В. Ильина ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2019. - 43 с. : рис. - Библиогр.: с. 42 (2 назв.). - ISBN 978-5-8088-1434-9 : Б. ц. - Текст : непосредственный.	5
004.7 К 95	Кучин, Николай Валентинович (доц.). Многоуровневые системы и облачные вычисления : учебное пособие / Н. В. Кучин, А. Ю. Молчанов ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2018. - 136 с. : рис. - Библиогр.: с. 133 (14 назв.). - ISBN 978-5-8088-1250-5 : Б. ц. - Текст : непосредственный	4

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
www.intuit.ru	Национальный Открытый Университет "ИНТУИТ"

8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Мультимедийная лекционная аудитория	
3	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; Экзаменационные билеты; Задачи; Тесты.

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

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	– обучающийся глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	– обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – 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	Архитектура современных распределенных информационных систем и систем их защиты.	ПК-1.В.1
2	Функционал систем управления безопасностью классических и нового поколения	ПК-2.3.2
3	Государственные стандарты, регламентирующие	ПК-2.3.7

	функционирование систем управления безопасностью	
4	Структурные компоненты распределенных информационных систем. Особенности защиты информационных ресурсов и процессов	ПК-2.У.4
5	Компоненты концептуальной модели ИБ. Графическая схема концептуальной модели системы ИБ.	ПК-2.У.5
6	Основные федеральные законы в области защиты информации	ПК-3.В.1
7	Объект и предмет защиты. Основные свойства информации как предмета защиты. Характерные особенности секретной и конфиденциальной информации	ПК-4.З.2
8	Объекты угроз ИБ. Понятие угрозы информации. Основные источники угроз защищаемой информации. Портрет злоумышленника	ПК-4.З.4
9	Уголовная ответственность: предусмотренная при неправомочном использовании информации критической информационной инфраструктуры	ПК-7.У.1
10	Охарактеризуйте свойства информации. Что такое признаковая информация? Почему семантическая информация по отношению к признаковой является вторичной? Какие признаки объектов являются демаскирующими?	ПК-9.З.2
11	Основные способы неправомерного овладения конфиденциальной информацией	ПК-10.З.2
12	Что такое утечка конфиденциальной информации? Как осуществляется утечка конфиденциальной информации?	ПК-10.У.1
13	Классы защищенности информационных систем	ПК-10.У.2
	Понятия доступности, целостности и конфиденциальности информации. Способы их обеспечения	ПК-10.В.2
14	Понятие кибератаки. Что такое окно опасности? Какие события происходят во время существования окна опасности?	ПК-11.З.1
15	Вектор угроз и его составляющие	ПК-11.З.2
16	Профиль защиты. Приведите стандарты, которые регламентируют разработку профилей защиты. Каково содержание задания по безопасности?	ПК-11.У.1
17	Классифицируйте угрозы ИБ РФ для личности, для общества, для Государства по общей направленности	ПК-1.В.1
18	Критическая информационная инфраструктура. Объекты КИИи субъекты КИИ	ПК-2.З.2
19	Управление рисками. Методики управлению рисками	ПК-2.З.7
20	Каналы утечки информации, Что такое технический канал утечки информации? Охарактеризуйте случайный и организованный канал утечки информации	ПК-2.У.4
21	Направления повседневной деятельности системного администратора, офицера по безопасности, обеспечивающие поддержание работоспособности ИС, а также состав рабочей группы по разработке и внедрению политик информационной безопасности	ПК-2.У.5 ПК-1.В.1
22	Информационные ресурсы ФСТЭК для разработчиков, администраторов и экспертов в сфере информационной	ПК-3.В.1

	безопасности	
23	Вредоносное программное обеспечение, Дайте определение «бомбы», «червя», «вируса». Какие негативные последствия в функционировании ИС вызывает вредоносное ПО?	ПК-4.З.2
24	Что такое идентификация? Дайте толкование понятия «аутентификация». Из-за каких причин затруднена надежная идентификация?	ПК-7.У.1
25	Средств защиты информации (СЗИ), их классификация. Классы защищенности СЗИ.	ПК-9.З.2
26	Особенности защиты биометрической информации	ПК-10.З.2
27	Системы контроля и управления доступом. Что такое матрица доступа? Какая информация анализируется при принятии решения о предоставлении доступа?	ПК-10.У.1
28	Системы протоколирования. Прокомментируйте особенности применения данного сервиса безопасности. Какие средства автоматизации существуют для мониторинга событий безопасности?	ПК-11.З.2 ПК-1.В.1
29	Основная задача аудита, как сервиса безопасности. Функциональность SIEM-систем?	ПК-11.У.1
30	Экранирование как сервис безопасности РИС. Что такое firewall и как он функционирует?	ПК-11.У.1
31	Для каких целей служит сервис анализа защищенности? В чем заключается специфика управления, как сервиса безопасности?	ПК-1.В.1
32	Какие нормативные акты и стандарты регламентируют деятельность по поверке (оценке) уровня защищенности? Что такое оценочный уровень доверия?	ПК-4.З.2

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
	Учебным планом не предусмотрено	

Перечень тем для курсового проектирования/выполнения курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для курсового проектирования/выполнения курсовой работы

№ п/п	Примерный перечень тем для курсового проектирования/выполнения курсовой работы
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
1	К какой разновидности моделей управления доступом относится модель Белла-Ла Падулы? а) модель дискреционного доступа; б) модель мандатного доступа;	ПК-2.З.2

	в) ролевая модель.	
1	Как называются угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.?	ПК-4.З.2
3	К каким мерам защиты относится политика безопасности? а) к административным; б) к законодательным; в) к программно-техническим; г) к процедурным.	ПК-1.В.1
4	В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу? а) ACL; б) списки полномочий субъектов; в) атрибутные схемы.	ПК-2.З.2
5	Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений? а) целостность; б) апеллируемость; в) доступность; г) конфиденциальность; д) аутентичность	ПК-2.З.2
6	К основным принципам построения системы защиты АИС относятся: а) открытость; б) взаимозаменяемость подсистем защиты; в) минимизация привилегий; г) комплексность; д) простота	ПК-7.У.1
7	Какие из следующих высказываний о модели управления доступом RBAC справедливы? а) с каждым субъектом (пользователем) может быть ассоциировано несколько ролей; б) роли упорядочены в иерархию; в) с каждым объектом доступа ассоциировано несколько ролей ; г) для каждой пары «субъект-объект» назначен набор возможных разрешений	ПК-9.З.2
8	. Диспетчер доступа... а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа; б) ... использует атрибутные схемы для представления матрицы доступа; в) ... выступает посредником при всех обращениях субъектов к объектам; г) ... фиксирует информацию о попытках доступа в системном журнале;	ПК-3.В
9	Какие предположения включает неформальная модель нарушителя? а) о возможностях нарушителя; б) о категориях лиц, к которым может принадлежать нарушитель; в) о привычках нарушителя; г) о предыдущих атаках, осуществленных нарушителем; д) об уровне знаний нарушителя	ПК-4.З.4

10	Что представляет собой доктрина информационной безопасности РФ? а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности; б) федеральный закон, регулирующий правоотношения в области информационной безопасности; в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов; г) совокупность официальных взглядов на цели, задачи, принципы и основные на- правления обеспечения информационной безопасности Российской Федерации	ПК-4.З.4
11	К какому виду мер защиты информации относится утвержденная программа работ в области безопасности? а) политика безопасности верхнего уровня; б) политика безопасности среднего уровня; в) политика безопасности нижнего уровня; г) принцип минимизации привилегий; д) защита поддерживающей инфраструктуры.	ПК-2.З.7
12	Какие из перечисленных ниже угроз относятся к классу преднамеренных? а) заражение компьютера вирусами; б) физическое разрушение системы в результате пожара; в) отключение или вывод из строя подсистем обеспечения функционирования вы- числительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.); г) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации; д) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; е) вскрытие шифров криптозащиты информации	ПК-2.У.4 ПК-2.У.5

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:

- Архитектура распределенных ИС
- Особенности защиты информации в РИС
- Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС
- Защита информации на уровне подсистемы управления
- Защита информации в каналах связи
- Особенности защиты информации в распределенных базах данных

.

11.2. Методические указания для обучающихся по участию в семинарах - *учебным планом не предусмотрено*

11.3. Методические указания для обучающихся по прохождению практических занятий - *учебным планом не предусмотрено*

.

11.4. 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

Лабораторная работа № 1 «Разработка модели угроз безопасности информации»

Цель лабораторной работы № 1: Построение различных моделей, отображающих архитектуру автоматизированной системы и ограничений доступа к информации. Проведение анализа мест и видов утечки информации. Оценка угроз, уязвимостей и степени защищенности информации.

Задание к лабораторной работе №1

1) Выполнить оценку актуальности разрабатываемой информационной системы
2) Провести структурный системный анализ бизнес-процессов предметной области. Построить диаграммы IDEF0 (AS-IS), DFD (AS-IS), (при необходимости – IDEF3 (AS-IS).
3) Описать разработанные диаграммы
4) Выделить активы, подлежащие информационной защите
5) Построить модель угроз разрабатываемой информационной системы
6) Построить модель нарушителя
7) Сформировать реестр актуализированных угроз для каждого актива
8) Сформировать векторы уязвимостей. Оценить возможные риски
9) Оценить степень защищенности информации

https://pro.guap.ru/get-task/cac51c01f6ef8be85769724d13573b9a

Структура и форма отчета о лабораторной работе

Отчет по лабораторным работам должна отражать не факт спроектированной системы защиты, а процесс проектирования, показывающий всю работу над проектом начиная от полученного исходного материала и наброска будущей защищенной информационной системы и заканчивая разработанным и протестированным программным пакетом, с обоснованием всех принятых в процессе проектирования решений.

Требования к оформлению отчета о лабораторной работе

В содержании должна быть отражена структура отчета. Введение должно характеризовать ту сферу человеческой деятельности, для которой будет проектироваться система защиты информации. При описании диаграмм должны быть изложены основные функциональные возможности будущей системы защиты информации, а также виды информации которые придется хранить и обрабатывать для достижения поставленной цели. В последующих лабораторных работах должны быть изложены этапы конструирования и функционирования программно-технических устройств защиты информации и технических объектов от несанкционированного доступа.

Лабораторная работа № 2 «Формирование структуры базы данных РИС»

Цель лабораторной работы: Спроектировать логическую и физическую ERD проектируемой (защищаемой) информационной системы.

Задание к лабораторной работе

1) На основании результатов системного анализа предметной области, полученных в лабораторной работе № 1 спроектировать архитектуру информационной системы

2) По DFD-модели (To-Be) составить таблицу соответствия внешних сущностей и накопителей таблицам базы данных (логический уровень)

3) Привести таблицы базы данных (логический уровень) в 3НФ (3 нормальную форму)
4) Установить связи между таблицами, типы связей в отчете описать
5) Разработать ER-диаграмму физического уровня
6) Оформить отчет по лабораторной работе.
В содержании должна быть отражена структура отчета.
https://pro.guap.ru/get-task/86f2a4558683e34c270a760f15b2ab1d

Лабораторная работа № 3 «Оценка и приоритизация рисков»

Цель лабораторной работы: Оценка защищенности информационной системы и приоритизация рисков ИБ.

Задание к лабораторной работе

1) На основании предположений безопасности, при учете угроз и имеющихся уязвимостей (модели угроз, полученной в лабораторных работах № 1-2) сформулировать цели безопасности, определить класс и категорию защищенности информационной (автоматизированной) системы.
2) Руководствуясь ГОСТ Р ИСО/МЭК ТО 13335, ГОСТ Р ИСО/МЭК 17799 и ГОСТ Р ИСО/МЭК 27001 выполнить априорную оценку и приоритизацию рисков, а также соблюдение законодательных и нормативных актов для рассматриваемой информационной системы (Для оценки рекомендуется использовать программное средство MICROSOFT SECURITY ASSESSMENT TOOL) https://www.microsoft.com/ru-ru/download/details.aspx?id=12273)

3) Результаты экспертной оценки рисков ИБ, полученные на предыдущем шаге использовать для формирования рекомендаций по приоритизации рисков

4) Провести оценку защищенности эксплуатируемой (AS-IS) и проектируемой (To-Be) информационной системы с учетом адаптации правил политик информационной безопасности (красных кружков в экспертной оценке не должно остаться).
5) Оформить отчет по лабораторной работе.

В содержании должна быть отражена структура отчета.
https://pro.guap.ru/get-task/9372943330e90d0af0d0974d8a9ec9d4

Лабораторная работа № 4 «Сбор логов событий информационной безопасности в AirSIEM»

Цель лабораторной работы № 4: разработать систему, которая позволяет анализировать регистрируемые в защищаемой инфраструктуре события, поступающие от различных источников, и обнаруживать атаки/сценарии атак/подозрительные действия/отклонения от нормы, формируя при необходимости соответствующие инциденты безопасности.

Задание к лабораторной работе №4

1) Развернуть SIEM-экосистему, используя проект AirSIEM (образ диска содержит AirSIEM, развернуую на Windows 7)
2) Развернуть AirSIEM, используя на Windows 10)

3) Реализовать подсистему сбора и хранения поступающих событий безопасности;
4) Оформить отчет по лабораторной работе.

Лабораторная работа № 5 Разработка Web-клиента мониторинга исключений в распределенной информационной системе

Цель работы: Изучить принципы построения MVC-решений, позволяющих распределить бизнес-логику в распределенных информационных системах, научиться использовать методы проектирования приложений доступа к данным, базируясь на принципах Model-First. Освоить механизмы Entity Framework для проектированияWeb-клиентов РИС.
Задание к лабораторной работе

1) Изучить материалы лекций размещенные в личном кабинете.

2) В соответствии с заявленной в лекциях функциональностью, разработать Web-клиент, использующий ASP.NET Core MVC подходы разработки распределенных систем.

3) Web-клиент должен обеспечивать возможность удаленного мониторинга таблицы UserExceptions разработанной ранее архитектуры БД, а также поддержку вызова CRUD-операций (create, read, update, delete) над данной таблицей.

4) Локализовать интерфейс Web-клиента (на русском языке должны бвть все его элементы)

5) Разработать дополнительный функционал проекта в соответствии с индивидуальным вариантом.

6) Оформить отчет по лабораторной работе, содержащий: титульный лист, название, номер и цель работы, постановку задачи, алгоритм решения для каждого программного модуля, листинг программных модулей, распечатку результатов, распечатку изображения форм, используемых в программе

11.5. Методические указания для обучающихся по прохождению курсового проектирования/выполнения курсовой работы *учебным планом не предусмотрено*

11.6. 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 обучающихсяявляются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

11.7. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

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

11.8. Методические указания для обучающихся по прохождению промежуточной аттестации.

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

– зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

– дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с 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