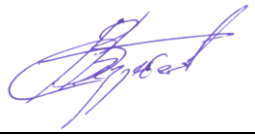
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

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

«Управление информационной безопасностью»
(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 2021 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 «Управление информационной безопасностью» 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-2 «Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности»

ОПК-3 «Способен разрабатывать проекты организационно-распорядительных документов по обеспечению 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 формированием необходимых теоретических и практических знаний, позволяющих проводить комплексный анализ защищенности и инструментальный мониторинг объекта защиты.

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

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

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Цель преподавания дисциплины заключается в формировании необходимого минимума специальных теоретических и практических знаний, позволяющих проводить комплексный анализ защищенности и инструментальный мониторинг объекта защиты, грамотно эксплуатировать программно-аппаратные средства защиты с учетом специфики существующих угроз информации.

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 достижениякомпетенции
Общепрофессиональные компетенции	ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2.З.5 знать назначение комплексной системы защиты информации, принципыееорганизации и этапы разработки ОПК-2.З.6 знать требования к системамкомплексной защиты информации ОПК-2.У.5 уметь разрабатывать модели угроз и нарушителей информационной безопасности информационных систем ОПК-2.В.4 владеть навыками участия в организации комплексной системы защиты объекта
Общепрофессиональные компетенции	ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ОПК-3.З.1 знать основы отечественных и зарубежных стандартов вобласти сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов ОПК-3.З.2 знать правила

		создания технического задания на создание подсистем безопасности информационных систем ОПК-3.З.3 знать основные угрозы безопасности информации и модели нарушителя в информационных системах ОПК-3.З.4 знать основныенормативные правовые акты в области обеспечения информационной безопасности ОПК-3.З.5 знать нормативные методические документыФСБ России в области защиты информации ОПК-3.З.6 знать нормативные методические документыФСТЭК России в областиинформационной безопасности ОПК-3.У.1 уметь разрабатывать техническиезадания на создание подсистем обеспечения информационной безопасности ОПК-3.У.2 уметь проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности ОПК-3.У.3 уметь разрабатывать проекты нормативных материалов, регламентирующих работупо защите информации ОПК-3.У.4 уметь разрабатывать нормативно-методические материалы по регламентации системы организационной защитыинформации ОПК-3.У.5 уметь разрабатывать организационно-распорядительнуюдокументацию по обеспечению информационной безопасности ОПК-3.В.1 владеть навыками разработки политик безопасности различных уровней ОПК-3.В.2 владеть навыками расчета и управления рисками информационной безопасности, навыкамиразработки положения о применимости механизмовконтроля в контексте управления рисками информационной безопасности ОПК-3.В.3 владеть правилами построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости исроков реализации ОПК-3.В.4 владеть навыками работы с нормативными правовымиактами в области информационной безопасности

Общепрофессиональные компетенции	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-4.З.3 знать методы анализа и обоснования выбора решений по обеспечению требуемогоуровня безопасности информационных систем
Общепрофессиональные компетенции	ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатыватьрезультаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	ОПК-5.З.4 знает порядокорганизации процесса исследования эффективности системы управления ИБ ОПК-5.З.5 знать нормативные и методические материалы в сфере информационной безопасности ОПК-5.У.3 умеет формализовать задачи анализа безопасности информационных систем, разрабатывать методики исследования и применять инструментальные средства анализа безопасности ОПК-5.В.5 владеет навыками обработки, оценки и представления результатов исследования эффективности решений по управлению информационной безопасностью

2. Место дисциплины в структуре ОП

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

– «Теория построения инфокоммуникационных систем и сетей»,

– «Программно-аппаратные средства защиты информации в инфокоммуникационных системах и сетях»,

– «Защищенные информационные системы».

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

		№3
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	3/ 108	3/ 108
Из них часов практической подготовки		
Аудиторные занятия, всего час.	34	34
в том числе:		
лекции (Л), (час)	17	17
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	17	17
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)	36	36
Самостоятельная работа, всего (час)	38	38
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 3					
Раздел 1. Общие вопросы организации управления информационной безопасностью	4		4		10
Раздел 2. Создание системы управления информационной безопасностью на предприятии	6		8		12
Раздел 3. Анализ состояния информационной безопасности IT-инфраструктуры	6		5		12
Текущий контроль	1				4
Итого в семестре:	17		17		38
Итого	17	0	17	0	38

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	**Раздел 1. Общие вопросы организации управления информационной безопасностью** Тема 1.1. Концепция управления информационной безопасностью. Цели и задачи управления информационной безопасностью. Архитектура системы обеспечения информационной безопасности. Роль политики безопасности в задачах управления информационной безопасностью. Тема 1.2. Стандарты управления информационной безопасностью. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799, их основные положения. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования" Сертификация систем управления информационной безопасностью на соответствие ISO 27001.
2	**Раздел 2. Создание системы управления информационной безопасностью на предприятии** Тема 2.1. Системы управления информационной безопасностью. Архитектура построения систем управления информационной безопасностью. Структура и функции систем управления информационной безопасностью. Тема 2.2. Этапы создания системы управления ИБ. Категорирование активов компании. Оценка защищенности информационной системы компании. Оценка информационных рисков. Тема 2.3. Методика оценки рисков информационной безопасности компании. Управление рисками. Основные понятия. Метод оценки рисков на основе модели угроз и уязвимостей. Метод оценки рисков на основе модели информационных потоков. Качественные методики управления рисками. Количественные методики управления рисками. Тема 2.4. Управление средствами защиты информации.
3	**Раздел 3. Анализ состояния информационной IT-инфраструктуры** Тема 3.1. Методы анализа состояния информационной безопасности. Аудит состояния информационной безопасности. Методы оценивания информационной безопасности. Способы анализа результатов аудита информационной безопасности. Метрики оценки оценивания информационной безопасности Тема 3.2. Методы оценки эффективности проводимых мероприятий. Тема 3.3. Средства управления информационной безопасностью. Программно-аппаратные средства управления безопасностью

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 3				
1	Разработка модели угроз безопасности информации	4	2	1
2	Формирование заданий по безопасности и SIEM-экосистемы	4	2	2
3	Сбор логов событий информационной безопасности в AirSIEM	4	2	2
4	Регистрация и анализ инцидентов в AirSIEM	5	3	3
Всего		17		

4.5. Курсовое проектирование/ выполнение курсовой работы

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 3, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	16	16
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	6	6
Домашнее задание (ДЗ)	16	16
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)		
Всего:	38	38

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 39	SIEM-системы в управлении информационной безопасностью : учебное пособие / С. В. Беззатеев, С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2021. - 131 с. : рис., табл. - Библиогр.: с. 128- 130 (28 назв.). - ISBN 978-5-8088-1676-3 : Б. ц. - Текст : непосредственный	4
004 Ф 76	Защита распределенных информационных систем : учебно-методическое пособие / С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2022. - 55 с. : рис., табл. - Библиогр.: с. 54 (10 назв.). - Б. ц. - Текст : непосредственный.	5
004 Ф 76	Методы машинного обучения в задачах обеспечения информационной безопасности : учебное пособие / С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2023. - 136 с. : рис. - Библиогр.: с. 131 - 133 (29 назв.). - ISBN 978-5-8088-1822-4 : Б. ц. - Текст : непосредственный.	5
681.5 О-75	Основы теории управления [Текст]: методические указания по выполнению лабораторных работ / С.Петерб. гос. ун-т аэрокосм. приборостроения; сост. Г. С. Бритов. - СПб. : Изд-во ГУАП, 2015. - 32 с.	77
004 М 87	Мошак Н. Н. Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие / Н.Н. Мошак, Т. М. Татарникова. приборостроения. - СПб.: Изд-во ГУАП, 2014. - 121 с.	40
004 М 48	Мельников, В. П. Защита информации [Текст]: учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; ред. В. П.Мельников. - М.: Академия, 2014. - 304 с.	10
004 Ш 22	Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для СПО / В. Ф. Шаньгин. - М.: ФОРУМ: ИНФРА-М, 2016. - 416 с.	10

http://znanium.com/catalog.php?bookinfo=423927	Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.	
http://znanium.com/catalog.php?bookinfo=489084	Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с.:	

7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
http://www.iso27000.ru/chitalnyi-zai/upravlenieinformacionnoi-bezopasnostyu/praktikaupravleniya-informacionnoi-bezopasnostyu	Практика управления информационной безопасностью
http://www.kachest-vo.ru/index.php?catid=4:it&id=67:ib-upravlenie&Itemid=18&option=com_content&vie w=article	Практический подход к построению системы управления Информационной безопасностью
http://www.ict.edu.ru/catalog/index.php?a=nav&c=getForm&d=light&id_res=1935&r=navDesc	Журнал "Защита информации. Конфидент"

8. Перечень информационных технологий

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

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
1	Операционная система MS Windows
2	Пакет MS Office
3	Среда разработки MS Visual Studio
4	Учебный проект AirSIEM https://github.com/fisher85/AirSIEM
5	Исходный код ядра корреляции - https://github.com/fisher85/AirSIEM/tree/master/AirSIEM

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

Перечень используемых информационно-справочных системпредставлен 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	52-48

10. Оценочные средства для проведения промежуточной аттестации

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

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Экзамен	Список вопросов к экзамену. Тесты

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 15. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 15 –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 16.

Таблица 16 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
1	Цели и задачи управления информационной безопасностью	ОПК-2.З.5 ОПК-2.З.6
2	Архитектура системы обеспечения информационной безопасности Роль политики безопасности в задачах управления информационной безопасностью.	ОПК-2.У.5 ОПК-2.В.4 ОПК-3.З.1
3	Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799, основные положения.	ОПК-3.З.2 ОПК-3.З.3
4	Международный стандарт ISO/IEC 27001:2005 «Системы управления информационной безопасности. Требования».	ОПК-3.З.4 ОПК-3.З.5
5	Сертификация систем управления информационной безопасностью на соответствие ISO 27001.	ОПК-3.З.6 ОПК-3.У.1
6	Структура и функции системы управления информационной безопасностью	ОПК-3.У.2 ОПК-3.У.3
7	Политика безопасности и ее роль в управлении информационной безопасностью	ОПК-3.У.4 ОПК-3.У.5
8	Этапы создания системы управления ИБ.	ОПК-3.В.1
9	Категорирование активов компании.	ОПК-3.В.2
10	Оценка защищенности информационной системы компании.	ОПК-3.В.3 ОПК-3.В.4
11	Оценка информационных рисков.	ОПК-4.З.3
12	Методика оценки рисков информационной безопасности компании.	ОПК-5.З.4 ОПК-5.З.5
13	Управление рисками. Основные понятия.	ОПК-5.У.3
14	Метод оценки рисков на основе модели угроз и уязвимостей.	ОПК-5.В.5
15	Метод оценки рисков на основе модели информационных потоков.	
16	Качественные методики управления рисками.	
17	Количественные методики управления рисками.	
18	Управление средствами защиты информации.	
19	Правовые основы аудита информационной безопасности	
20	Место и роль аудита в управлении информационной безопасности	
21	Методология проведения аудита информационной безопасности	

22	Менеджмент аудита информационной безопасности	
23	Методы оценки эффективности информационной безопасности	
24	Способы анализ результатов аудита информационной безопасности	
25	Нормативно-технические документы аудита информационной безопасности	
26	Виды контроля состояния информационной безопасности объектов	
27	Методы анализа состояния информационной безопасности	

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 работыпредставлены 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 тестированияпредставлены 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; в) ролевая модель.	ОПК-4.З.3
2.	Как называются угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.?	ОПК-5.У.3
3.	К каким мерам защиты относится политика безопасности? а) к административным; б) к законодательным; в) к программно-техническим; г) к процедурным.	ОПК-2.З.5
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.	ОПК-3.В.2
5.	Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений? а) целостность;	ОПК-2.З.6

	б) апеллируемость; в) доступность; г) конфиденциальность; д) аутентичность	
6.	К основным принципам построения системы защиты АИС относятся: а) открытость; б) взаимозаменяемость подсистем защиты; в) минимизация привилегий; г) комплексность; д) простота	ОПК-2.З.5
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	ОПК-2.У.5
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;	ОПК-5.В.5
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	ОПК-2.З.6
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 направления обеспечения информационной безопасности Российской Федерации	ОПК-2.З.6
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.	ОПК-3.У.2
12.	Какие из перечисленных ниже угроз относятся к классу преднамеренных?	ОПК-3.З.2

	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	

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

11. Методические указания для обучающихся по освоению дисциплины

11.1. Методические указания для обучающихся по освоению лекционного материала.

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимися лекционного материала:

– получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;

– получение опыта творческой работы совместно с преподавателем;

– развитие профессионально-деловых качеств, любви к предмету и самостоятельного творческого мышления.

– появление необходимого интереса, необходимого для самостоятельной работы;

– получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;

– научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);

– получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

Раздел 1. Общие вопросы организации управления информационной безопасностью

Тема 1.1. Концепция управления информационной безопасностью. Тема 1.2.

Стандарты управления информационной безопасностью.
Раздел 2. Создание системы управления информационной безопасностью на предприятии.
Тема 2.1. Системы управления информационной безопасностью.Тема 2.2.
Этапы создания системы управления ИБ.
Тема 2.3. Методика оценки рисков информационной безопасности компании.Тема 2.4.
Управление средствами защиты информации.
Раздел 3. Анализ состояния информационной безопасности IT-инфраструктуры
Тема 3.1. Методы анализа состояния информационной безопасности.Тема 3.2.
Методы оценки эффективности проводимых мероприятий. Тема 3.3. Средства управления информационной безопасностью.

Структура предоставления материала каждой лекции состоит из:

– вступления (введения), где определяется тема, план и цель лекции. Обосновывается предмет лекции и ее актуальность, основная идея (проблема, центральный вопрос), связь с предыдущими и последующими занятиями, основные вопросы лекции;

– изложения содержания, где реализуется научное содержание темы, все главные вопросы, приводится система доказательств с использованием наиболее целесообразных методических приемов. В ходе изложения применяются все формы и способы суждения, аргументации и доказательства. Все доказательства и разъяснения направлены на достижение поставленной цели, раскрытие основной идеи, содержания и научных выводов. Каждый учебный вопрос заканчивается краткими выводами, логически подводящими студентов к следующему вопросу лекции. Количество вопросов в лекции, как правило, от двух до четырех;

– заключения, где обобщаются в кратких формулировках основные идеи лекции, логически завершая ее как целостное изучение темы. В нем могут даваться рекомендации о порядке дальнейшего изучения основных вопросов лекции самостоятельно по указанной литературе.

11.2. Методические указания для обучающихся по выполнению лабораторных

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 с точки зрения инженера безопасности информации. Построить диаграммы IDEF0 (AS-IS), DFD (ASIS), (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

.

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. 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

Требования к оформлению отчета о лабораторной работе

- Отчет по лабораторной работе предоставляется в печатном/или электронном виде;
- должна соответствовать структуре и форме отчета, представленной выше;
- Отчет по лабораторной работе должен иметь титульный лист (ГОСТ 7.32-2001 издания 2008 года) с названием и подписью студента(ов), который(ые) ее сделал(и) и оформил(и);
- Студент должен защитить ЛР. Отметка о защите должна находиться на титульном листе вместе с подписью преподавателя.

Ссылка на материалы ЛР1 -
https://pro.guap.ru/inside/professor/tasks/563990456001f9664c7e238a8297e45b/download

Лабораторная работа № 2 «Формирование заданий по безопасности и SIEM-экосистемы»

Цель лабораторной работы № 2: На основании формулированных целей безопасности сформировать профили защиты и задания по безопасности информационной системы и СЗИ, реализующих требуемый уровень защищенности системы. Развернуть SIEM-экосистему

Задание к лабораторной работе №2

1) На основании сформулированных целей безопасности сформировать профили защиты информационной (автоматизированной) системы и/или СЗИ.
2) В профилях защиты построить таблицы, которые взаимосвязывают Цели безопасности с угрозами и ПолИБ. Взаимосвязи обосновать и описать.
3) Сформулировать функциональные требования, требования доверия и требования к среде
4) Разработать задание по безопасности. Выделить правила безопасности, реализованные в технических политиках безопасности, которые предстоит реализовать в подсистеме анализа (корреляций) SIEM-системы.
5) Развернуть SIEM-экосистему, используя проект AirSIEM https://github.com/fisher85/AirSIEM
6) Исходный код ядра корреляции - https://github.com/fisher85/AirSIEM/tree/master/AirSIEM
7) Оформить отчет по лабораторной работе

Структура и форма отчета о лабораторной работе

- Постановка задачи;
- Входные и выходные данные;
- Содержание этапов выполнения;
- Обоснование полученного результата (вывод);
- Список используемой литературы

Требования к оформлению отчета о лабораторной работе

- Отчет по лабораторной работе предоставляется в печатном/или электронном виде;
- должна соответствовать структуре и форме отчета, представленной выше;
- Отчет по лабораторной работе должен иметь титульный лист (ГОСТ 7.32-2001 издания 2008 года) с названием и подписью студента(ов), который(ые) ее сделал(и) и оформил(и);
- Студент должен защитить ЛР. Отметка о защите должна находиться на титульном листе вместе с подписью преподавателя

Ссылка на материалы ЛР2 - https://pro.guap.ru/inside/professor/tasks/130862/show

Лабораторная работа № 3 «Сбор логов событий информационной безопасности в AirSIEM»

Цель лабораторной работы № 3: 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 №3

1) Сформировать технические политики ИБ
2) На основании разработанных политик информационной безопасности, профилей защиты и заданий по безопасности информационной (автоматизированной) системы и/или СЗИ, разработать архитектуру SIEM-системы
3) Реализовать подсистему сбора и хранения поступающих событий безопасности;
4) Оформить отчет по лабораторной работе.

Структура и форма отчета о лабораторной работе

- Постановка задачи;
- Входные и выходные данные;
- Содержание этапов выполнения;
- Обоснование полученного результата (вывод);
- Список используемой литературы

Требования к оформлению отчета о лабораторной работе

- Отчет по лабораторной работе предоставляется в печатном/или электронном виде;
- должна соответствовать структуре и форме отчета, представленной выше;
- Отчет по лабораторной работе должен иметь титульный лист (ГОСТ 7.32-2001 издания 2008 года) с названием и подписью студента(ов), который(ые) ее сделал(и) и оформил(и);
- Студент должен защитить ЛР. Отметка о защите должна находиться на титульном листе вместе с подписью преподавателя

Ссылка на материалы ЛР3 - https://pro.guap.ru/inside/professor/tasks/0f0af0a0c82ee10e5162598d276781ca/download

Лабораторная работа № 4 «Регистрация и анализ инцидентов 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) Реализовать обработку и анализ зарегистрированных событий безопасности;
2) Разработать подсистему обнаружения атак и нарушений политик безопасности в реальном времени (близком к реальному времени);
3) Реализовать выявление и разбор инцидентов безопасности.

4) Оформить отчет по лабораторной работе.

Структура и форма отчета о лабораторной работе

- Постановка задачи;
- Входные и выходные данные;
- Содержание этапов выполнения;
- Обоснование полученного результата (вывод);
- Список используемой литературы

Требования к оформлению отчета о лабораторной работе

- Отчет по лабораторной работе предоставляется в печатном/или электронном виде;
- Должен соответствовать структуре и форме отчета, представленной выше;
- Отчет по лабораторной работе должен иметь титульный лист (ГОСТ 7.32-2001 издания 2008 года) с названием и подписью студента(ов), который(ые) ее сделал(и) и оформил(и);
- Студент должен защитить ЛР. Отметка о защите должна находиться на титульном листе вместе с подписью преподавателя

Ссылка на материалы ЛР4 -
https://pro.guap.ru/inside/professor/tasks/974b88d16917bf53a151b8f65a5d249c/download

11.3. Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся 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:

- Стандарты управления информационной безопасностью.
- Этапы создания системы управления ИБ.
- Методика оценки рисков информационной безопасности компании.
- Методы анализа состояния информационной безопасности.
- Методы оценки эффективности проводимых мероприятий.
- Средства управления информационной безопасностью.

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

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

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».

11.5. Методические указания для обучающихся по прохождению промежуточной

аттестации.

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