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

Кафедра № 51

УТВЕРЖДАЮ
Руководитель направления

доц.,к.т.н.,доц.
(должность, уч. степень, звание)
А.А. Овчинников
(инициалы, фамилия)

(подпись)
«19» __мая___ 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Инженерно-технические средства защиты информации»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.03.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности	Безопасность компьютерных систем
Форма обучения	очная

Санкт-Петербург – 2021

Лист согласования рабочей программы дисциплины

Программу составил (а)

Ст. преп.	19.05.2021	А.В. Афанасьева
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 51

«19» мая 2021 г., протокол №10

Заведующий кафедрой № 51

к.т.н.,доц.	19.05.2021	А.А. Овчинников
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Ответственный за ОП ВО 10.03.01(01)

доц.,к.т.н.,доц.	19.05.2021	А.А. Овчинников
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №5 по методической работе

доц.,к.т.н.,доц.	19.05.2021	О.И. Красильникова
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Аннотация

Дисциплина «Инженерно-технические средства защиты информации» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 10.03.01 «Информационная безопасность» направленности «Безопасность компьютерных систем». Дисциплина реализуется кафедрой «№51».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-3 «Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств защиты информации, способен к использованию и внедрению результатов исследований»

ПК-5 «Способен организовывать и проводить настройку программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты от несанкционированного доступа»

ПК-6 «Способен администрировать средства защиты информации прикладного и системного программного обеспечения»

Содержание дисциплины охватывает круг вопросов, связанных с реализацией требований политик безопасности при построении комплексной системы защиты информации.

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 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский »

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью преподавания дисциплины «Инженерно-технические средства защиты информации» является формирование у студентов знаний, умений и навыков по определению задач подсистемы инженерно-технической защиты информации в комплексной системе защиты информации объекта, разработке, внедрению и эксплуатации подсистемы инженерно- технической защиты информации, а также организации контроля эффективности подсистемы инженерно- технической защиты информации и выполнению основных операций контроля.

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-3 Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств защиты информации, способен к использованию и внедрению результатов исследований	ПК-3.У.1 умеет применять актуальную нормативную документацию в соответствующей области знаний
Профессиональные компетенции	ПК-5 Способен организовывать и проводить настройку программных, программно-аппаратных (в том числе крипто-графических) и технических средств и систем защиты от несанкционирован-ного доступа	ПК-5.У.1 умеет устанавливать и настраивать параметры сетевых протоколов, реализованных в телекоммуникационном оборудовании

Профессиональные компетенции	ПК-6 Способен администрировать средства защиты информации прикладного и системного программного обеспечения	ПК-6.З.2 знает принципы построения антивирусного программного обеспечения ПК-6.В.1 владеет определением порядка установки программного обеспечения с целью соблюдения требований по защите информации ПК-6.В.2 владеет навыками по выполнению работ по обнаружению вредоносного программного обеспечения

2. Место дисциплины в структуре ОП

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

- Основы информационной безопасности;
- Документоведение.

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

- Защита информационных процессов в компьютерных системах;
- Проектирование систем обеспечения ИБ.

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
		№7
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	3/ 108	3/ 108
Из них часов практической подготовки	34	34
Аудиторные занятия, всего час.	51	51
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)		
экзамен, (час)	36	36
Самостоятельная работа, всего (час)	21	21
***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 7					
Раздел 1. Принципы построения комплексной системы защиты	2		4		4
Раздел 2. Система менеджмента информационной безопасности. Политики безопасности	4		6		3
Раздел 3.Жизненный цикл проекта создания системы информационной безопасности	2		6		3
Раздел 4 Вредоносные программные продукты и защита от них	2		6		3
Раздел 5 Методики оценки состояния информационной безопасности	2		6		3
Раздел 6. Управление инцидентами	5		4		3
Текущий контроль			2		2
Итого в семестре:	17		34		21
Итого	17	0	34	0	21

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.Требования к системе защиты информации. Комплексность требований. Тема 1.2. Характеристики безопасности и способы их реализации.Тема 1.3. Метрики безопасности Тема 1.4. Методы системотехники. Тема 1.5. Роль моделей и моделирования.
2	Тема 2.1. Система менеджмента информационной безопасности. Тема 2.2. Учет требований регуляторов. Тема 2.3. Политики безопасности. Тема 2.4. Стандарты информационной безопасности. Стандарты серии 27000. Стандарт ГОСТ Р 15408 и его применение. Критерии соответствия. Тема 2.5. Аудит безопасности. Тема 2.6. Тестирование на проникновение
3	Тема 3.1. Жизненный цикл программного продукта и жизненный цикл системы информационной безопасности. Тема 3.2. Модели жизненного цикла: линейная,

	водопадная, спиральная, V-образная. Тема 3.3. Модель XP. Microsoft SDL. Тема 3.4. Контроль параметров безопасности программного продукта.
4	Тема 4.1. Вредоносные программы продукты и защита от них. Цели и варианты классификации зловредов. Жизненный цикл зловреда. Тема 4.2. Обнаружение и удаление зловреда. Политика превентивной защиты от зловредов. Стандарт ГОСТ Р 51188-98
5	Тема 5.1. Методики оценки состояния информационной безопасности. Тема 5.2. Активы, уязвимости, угрозы, риск.
6	Тема 6.1. Управление инцидентами. Тема 6.2. Социальная инженерия

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 7				
1	Настройки параметров безопасности ОС	2	2	1
2	Моделирование угроз. Метод CORAS	4	4	2
3	Модели угроз. Оценка значимости угроз	4	4	2
4	Виртуальная машина VirtualBox и особенности ее использования при исследовании вопросов информационной безопасности	4	4	2
5	Microsoft Software Development Lifecycle	4	4	3
6	Microsoft Attack Surface Analyzer	4	4	4
7	Утилиты М. Руссиновича	4	4	5
8	Управление рисками	4	4	5,6
	Защита отчетов, обсуждение результатов	4	4	
Всего		34	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 7, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	6	6
Подготовка лабораторных работ (ЛР)	9	9
Подготовка к текущему контролю успеваемости (ТКУ)	7	7
Всего:	21	21

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 7-11.

6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004 М 87-604316-ED	Мошак Н.Н. Защищенные инфотелеком-муникации. Анализ и синтез [Электронный ресурс]: монография/Н.Н. Мошак. – Электрон. Текстовые дан. – СПб.: Изд-во ГУАП, 2014. – 197 с.	40
004 М 87	Организация безопасного доступа к информационным ресурсам: учебное пособие / Н. Н. Мошак, Т. М. Татарникова. - СПб.:Изд-во ГУАП, 2014. - 121 с.	40
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://e.lanbook.com/view/book/850/	Кадино Э. Электронные системы охраны.ДМК Пресс, 2010.	
http://znanium.com/catalog.php?	Аверченков, В. И. Аудит	

bookinfo=453734	информационной безопасности [электронный ресурс]: учеб. пособие для вузов / В. И. Аверченков. – 2-е изд., стереотип. – М. : Флинта, 2011. – 269 с	
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=471787	Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.	

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

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

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

URL адрес	Наименование
http://securitypolicy.ru/index.php	Портал документов по информационной безопасности
http://fstec.ru/	Портал ФСТЭК
http://www.gostedu.ru/	Портал стандартов
http://анализ-риска.рф/content/iskusstvo-upravleniya-informacionnymi-riskami	Астахов А. Искусство управления информационными рисками 2009

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	Microsoft Office
2	Visio
3	VirtualBox

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	Лаборатория вычислительной техники	

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

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;

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
	– 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	Комплексность требований к системе защиты информации	ПК-3.У.1 ПК-5.У.1 ПК-6.З.2 ПК-6.В.1 ПК-6.В.2
2	Характеристики безопасности	
3	Способы реализации характеристик безопасности	
4	Метрики безопасности	
5	Методы системотехники	
6	Роль моделей и моделирования в задачах защиты информации	
7	Система менеджмента информационной безопасности	
8	Учет требований регуляторов	
9	Политики безопасности	
10	Стандарты информационной безопасности	
11	Стандарты серии 27000.	
12	Стандарт ГОСТ Р 15408 и его применение	
13	Аудит безопасности Тестирование на проникновение Жизненный цикл	
14	Жизненный цикл системы информационной безопасности	
15	Линейная модель жизненного цикла	
16	Водопадная модель жизненного цикла	
17	Спиральная модель жизненного цикла	
18	V-образная модель жизненного цикла	
19	Политики безопасности	
20	Стандарты информационной безопасности	
21	Модель XP	
22	Microsoft SDL	
23	Контроль параметров безопасности программного продукта	
24	Цели и варианты классификации зловредов	
25	Жизненный цикл зловреда	
26	Обнаружение и удаление зловреда	
27	Стандарт ГОСТ Р 51188-98	
28	Политика превентивной защиты от зловредов	
29	Активы, уязвимости, угрозы, риск.	
30	Методики оценки состояния информационной безопасности	
31	Управление инцидентами	
32	Социальная инженерия	

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
	не предусмотрено	

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

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

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

11. Методические указания для обучающихся по освоению дисциплины

Целью дисциплины является – получение студентами необходимых знаний, умений и навыков по определению задач подсистемы инженерно-технической защиты информации в комплексной системе защиты информации объекта, разработке, внедрению и эксплуатации подсистемы инженерно-технической защиты информации, а также организации контроля эффективности подсистемы инженерно-технической защиты информации и выполнению основных операций контроля.

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. Принципы построения комплексной системы защиты информации

Тема 1.1.Требования к системе защиты информации. Комплексность требований. Тема 1.2. Характеристики безопасности и способы их реализации.

Тема 1.3. Метрики безопасности Тема 1.4. Методы системотехники.

Тема 1.5. Роль моделей и моделирования.

Раздел 2. Система менеджмента информационной безопасности. Политики безопасности

Тема 2.1. Система менеджмента информационной безопасности. Тема 2.2. Учет требований регуляторов.

Тема 2.3. Политики безопасности.

Тема 2.4. Стандарты информационной безопасности. Тема 2.5. Аудит безопасности.

Тема 2.6. Тестирование на проникновение.

Раздел 3.Жизненный цикл проекта создания системы информационной безопасности

Тема 3.1. Жизненный цикл программного продукта и жизненный цикл системы информационной безопасности.

Тема 3.2. Модели жизненного цикла: линейная, водопадная, спиральная, V-образная. Тема 3.3. Модель XP. Microsoft SDL.

Тема 3.4. Контроль параметров безопасности программного продукта.

Раздел 4 Вредоносные программные продукты и защита от них Тема 4.1. Вредоносные программы продукты и защита от них. Тема 4.2. Обнаружение и удаление зловреда.

Раздел 5 Методики оценки состояния информационной безопасности

Тема 5.1. Методики оценки состояния информационной безопасности. Тема 5.2. Активы, уязвимости, угрозы, риск.

Раздел 6. Управление инцидентами Тема 6.1. Управление инцидентами. Тема 6.2. Социальная инженерия

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

Вариант задания по каждой лабораторной работе обучающийся получает в соответствии с номером в списке группы. В соответствии с заданием обучающийся должен подготовить необходимые данные, получить от преподавателя допуск к выполнению лабораторной работы, выполнить указанную последовательность действий, получить требуемые результаты, защитить полученные результаты.

Структура и форма отчета о лабораторной работе

Отчет содержит следующие элементы:

1. Постановка задачи
2. Последовательность решения задачи
3. Полученные результаты и их анализ
4. Вывод о проделанной работе

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. [004.056.5 А 76 004] Аппаратно-программные средства защиты информации: методические указания к выполнению лабораторных работ №1-7/ С.-Петерб. гос. ун-т аэрокосм. приборостроения; сост.: А. В. Окатов, А. А. Овчинников. - СПб: ГОУ ВПО "СПбГУАП", 2009, 46 с. Кол-во экз. в библ. – 70.
2. [004.3 А 76 004] Аппаратные средства вычислительной техники: методические указания к выполнению лабораторных работ № 1 - 8/ С.-Петерб. гос. ун-т аэрокосм. приборостроения; сост.: А. В. Окатов, А. А. Овчинников. - СПб: ГОУ ВПО "СПбГУАП", 2009. - 39 с. Кол-во экз. в библ. – 76.
3. [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.

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.

Перечень тем для самостоятельного изучения:

- Метрики безопасности
- Методы системотехники.
- Система менеджмента информационной безопасности.
- Учет требований регуляторов.
- Стандарты информационной безопасности.
- Аудит безопасности.
- Тестирование на проникновение.
- Модели жизненного цикла: линейная, водопадная, спиральная, V-образная.
- Контроль параметров безопасности программного продукта.
- Обнаружение и удаление зловреда.
- Методики оценки состояния информационной безопасности.
- Активы, уязвимости, угрозы, риск.
- Управление инцидентами.
- Социальная инженерия

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. 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».

11.8. 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». 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