


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
проф., д.т.н., доц.
(должность, уч. степень, звание)
 С.В. Бездатсев
(подпись)

«24» июня 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Программно-аппаратная защита информации»
(Название дисциплины)

Код направления	10.05.05
Наименование направления/ специальности	Безопасность информационных технологий в правоохранительной сфере
Наименование направленности	Технологии защиты информации в правоохранительной сфере
Форма обучения	очная

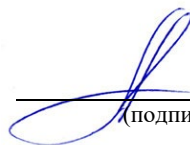
Санкт-Петербург– 2021 г.

Лист согласования рабочей программы дисциплины

Программу составил (а)

зав.каф., к.т.н., доц.

(должность, уч. степень, звание)

24.06.2021

(подпись, дата)

А.А. Овчинников

(инициалы, фамилия)

Программа одобрена на заседании кафедры № 51

«24» июня 2021 г, протокол №11

Заведующий кафедрой № 51

к.т.н., доц.

(уч. степень, звание)

24.06.2021

(подпись, дата)

А.А. Овчинников

(инициалы, фамилия)

Ответственный за ОП 10.05.05(01)

доц., к.т.н., доц.

(должность, уч. степень, звание)

24.06.2021

(подпись, дата)

В.А. Мыльников

(инициалы, фамилия)

Заместитель директора института №3 по методической работе

доц., к.э.н., доц.

(должность, уч. степень, звание)

24.06.2021

(подпись, дата)

Г.С. Армашова-Тельник

(инициалы, фамилия)

Аннотация

Дисциплина «Программно-аппаратная защита информации» входит в базовую часть образовательной программы подготовки обучающихся по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» направленность «Технологии защиты информации в правоохранительной сфере». Дисциплина реализуется кафедрой №51.

Дисциплина нацелена на формирование у выпускника

общефессиональных компетенций:

ОПК-1 «способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач»;

профессиональных компетенций:

ПК-1 «способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз»,

ПК-2 «способность применять технические и программно-аппаратные средства обработки и защиты информации»,

ПК-5 «способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного населения»,

ПК-6 «способность осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации».

Содержание дисциплины охватывает круг вопросов, связанных с изучением механизмов и практических методов защиты информации в компьютерных системах

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 дифференцированного зачета.

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 ознакомлении студентов с технологиями защиты информации, реализуемых современными программно-аппаратными средствами.

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

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-1 «способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач»:

знать – математический аппарат, применяемый в криптографической защите информации;
 уметь – строить модель нарушителя и прогнозировать на её основе уровень угроз информационной безопасности;
 владеть навыками – по применению методов моделирования информационных систем в задачах защиты информации;
 иметь опыт деятельности – по оценке возможных угроз для защищаемых объектов информатизации;

ПК-1 «способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз»:

знать – современные программно-аппаратные средства и технологии защиты информации;
 уметь – применять программные и технические средства системного, прикладного и специального назначения, в том числе средства защиты информации, составляющей государственную тайну;
 владеть навыками – программирования, администрирования и эксплуатации систем и применения инструментальных средств программирования в профессиональной деятельности;
 иметь опыт деятельности – в комплексном применении программных и технических средств системного, прикладного и специального назначения при решении конкретных задач по защите информации;

ПК-2 «способность применять технические и программно-аппаратные средства обработки и защиты информации»:

знать – современные базу программно-аппаратных и криптографических средств защиты информации;
 уметь – выбирать и применять программно-аппаратные и криптографические средства защиты информации в зависимости от условий задачи защиты информации;
 владеть навыками – решения задач выбора программно-аппаратных и криптографических средств защиты информации при известных условиях их применения;
 иметь опыт деятельности – в применении программно-аппаратных и криптографических средства защиты информации в зависимости от условий задачи защиты информации;

ПК-5 «способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного населения»:

знать – новые образцы программных комплексов, технических средств и информационных технологий, применяемых для защиты информации

уметь – выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств обработки и защиты информации

владеть навыками – эксплуатации и администрирования подсистемы обеспечения информационной безопасности на объекте;

иметь опыт деятельности – в настройке и обслуживании технических и программно-аппаратных средств обработки и защиты информации, эксплуатации и администрировании подсистемы обеспечения информационной безопасности на объекте;

ПК-6 «способность осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации»:

знать – основные уязвимости компьютерных систем;

уметь – использовать системы разграничения доступа к информации в компьютерных системах;

владеть навыками – по применению политик безопасности в подсистемах обеспечения информационной безопасности объекта информатизации;

иметь опыт деятельности - по администрированию подсистем обеспечения информационной безопасности объекта информатизации.

2. Место дисциплины в структуре ОП

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

- Программирование. Методы и технологии программирования
- Средства вычислительной техники
- Теория информации

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

- Методология защиты информации
- Защита информации в распределенных информационных системах
- Защита и обработка документов ограниченного доступа
- Технологии защиты электронных платежей

3. Объем дисциплины в ЗЕ/академ. час

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 1

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№6
1	2	3
Общая трудоемкость дисциплины, ЗЕ/(час)	3/ 108	3/ 108
Из них часов практической подготовки	27	27
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)		
Самостоятельная работа , всего (час)	93	93
Вид промежуточного контроля: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.)	Дифф. Зач.	Дифф. Зач.

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий

Разделы и темы дисциплины и их трудоемкость приведены в таблице 2.

Таблица 2. – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 6					
Раздел 1. Введение	1				3
Раздел 2. Программно-аппаратные средства реализации идентификации и аутентификации	4		10		10
Раздел 3. Программно-аппаратные средства реализации ограничения доступа	3		10		12
Раздел 4. Программно-аппаратные средства конфиденциальности, хранения информации	4		8		16
Раздел 5. Средства защиты программ	4		6		12
Текущий контроль					4
Итого в семестре:	17		34		57
Итого:	17	0	34	0	57

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 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Раздел 1. Введение. Предмет и задачи программно-аппаратной защиты информации. Основные понятия. Уязвимости компьютерных систем. Политика безопасности в компьютерных системах. Оценка защищенности. Механизмы защиты. Программно-аппаратные средства для реализации политики безопасности.
2	Раздел 2. Программно-аппаратные средства реализации идентификации и аутентификации Тема 2.1. Схемы идентификации и аутентификации. Одно- и

	<p>многофакторная аутентификация. Программно-аппаратные средства реализации протоколов идентификации и аутентификации:</p> <ul style="list-style-type: none"> – протоколы идентификации и аутентификации; – ОТР-токены. <p>Тема 2.2. Биометрическая идентификация и аутентификация пользователя.</p> <p>Биометрические характеристики. Реализация биометрических систем.</p>
3	<p>Раздел 3. Программно-аппаратные средства реализации ограничения доступа</p> <p>Тема 3.1. Система разграничения доступа к информации в компьютерной системе.</p> <p>Концепция построения систем разграничения доступа.</p> <p>Тема 3.2. Средства и методы ограничения доступа к файлам</p> <p>Организация доступа к файлам. Фиксация доступа к файлам.</p> <p>Доступ к данным со стороны процесса. Особенности защиты данных от изменения.</p> <p>Тема 3.3. Методы и средства ограничения доступа к компонентам ЭВМ</p> <p>Компоненты ПЭВМ. Способы защиты информации на съемных носителях. Организация прозрачного режима шифрования.</p> <p>Надежность средств защиты компонент.</p>
4	<p>Раздел 4. Программно-аппаратные средства конфиденциальности, хранения информации</p> <p>Тема 4.1. Программно-аппаратные средства шифрования.</p> <p>Аппаратные и программно-аппаратные средства криптозащиты данных. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования.</p> <p>Защита алгоритма шифрования.</p> <p>Тема 4.2. Инфраструктура открытых ключей (PKI).</p> <p>Аппаратные средства защиты в PKI-решениях. Хранения ключевой информации.</p> <p>Тема 4.3. Централизованная система управления средствами аутентификации и хранения ключевой информации пользователей.</p> <p>Требования к системе управления токенами. Комплексная система на базе единого персонального средства аутентификации и хранения ключевой информации.</p>
5	<p>Раздел 5. Средства защиты программ</p> <p>Тема 5.1. Защита программ от несанкционированного копирования</p> <p>Основные методы защиты от копирования.</p> <p>Привязка ПО к аппаратному окружению и физическим носителям как средство защиты от копирования ПО. Привязка программ к носителям. Физические метки и технология работы с ними.</p> <p>Привязка программ к жестким магнитным дискам. Привязка к внешним (добавляемым) элементам ПЭВМ. Использование дополнительных плат расширения. Методы «водяных знаков» и методы «отпечатков пальцев».</p> <p>Тема 5.2. Защита программных средств от исследования.</p> <p>Изучение и обратное проектирование ПО. Задачи защиты от изучения и способы их решения. Аспекты проблемы защиты от исследования. Методы противодействия дизассемблированию.</p> <p>Вирусы.</p>

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 4.

Таблица 4 – 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					

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 6				
1	Протоколы идентификации	2		2
2	Протоколы аутентификации	2		2
3	Программно-аппаратные средства разграничения доступа к программам и данным	2	1	3
4	Аппаратные устройства криптографической защиты данных серии КРИПТОН	2	2	4
5	Программно-аппаратные комплексы защиты информации от несанкционированного доступа	2	2	3
6	Программно-аппаратные комплексы для обеспечения информационной безопасности в локальной вычислительной сети	2	2	2,3
7	Программные комплексы для защиты данных на ПК	2	2	2,3
8	Аппаратные решения для выявления и предотвращения утечек конфиденциальной информации	4	4	2,3
9	Носители ключевой информации	2	2	4
10	Система Kerberos	4	4	4
11	Протокол SKIP управления криптоключами	4	2	4
12	Средства противодействия дизассемблированию	2	2	5
13	Защита программного обеспечения от копирования с помощью электронных ключей	4	4	5
Всего:		34	27	

4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 6, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	23	23
Расчетно-графические задания (РГЗ)	30	30
Подготовка к текущему контролю успеваемости (ТКУ)	4	4
Всего:	57	57

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

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 6-11.

6. Перечень основной и дополнительной литературы

6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основной литературы

Шифр	Библиографическая ссылка / URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004 Н 74	Новожилов, О. П. Архитектура ЭВМ и систем [Текст]: учебное пособие для бакалавров / О. П. Новожилов. - М. : Юрайт, 2015. - 527 с.	50
004 А 18	Авдеев, В. А. Периферийные устройства: интерфейсы, схемотехника, программирование [Текст]: учебное пособие / В. А. Авдеев. - М. : ДМК Пресс, 2014. - 848 с.	2
004 А 76	Аппаратные средства поддержки операционных систем [Текст]: методическое пособие / С.-Петербург. гос. ун-т аэрокосм. приборостроения; сост. Н. В. Кучин. - СПб.: Изд-во ГУАП, 2015. - 43 с.	86
	Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с.: http://znanium.com/catalog.php?bookinfo=489084	
	Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие /Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. http://znanium.com/catalog.php?bookinfo=503511	

	Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с. http://znanium.com/catalog.php?bookinfo=402686	
--	--	--

6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительной литературы

Шифр	Библиографическая ссылка/ URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004/М 87-604316-ED	Мошак Н. Н. Защищенные инфотелекоммуникации. Анализ и синтез [Электронный ресурс]: монография / Н. Н. Мошак; С.-Петербур. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - СПб.: Изд-во ГУАП, 2014. - 197 с.	
004 М 17	Максимов, Н. В. Архитектура ЭВМ и вычислительные системы [Текст]: учебник для СПО / Н. В. Максимов, Т. Л. Партыка, И. И. Попов. - 5-е изд., перераб. и доп. - М.: ФОРУМ : ИНФРА-М, 2014. – 512 с.	
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.	
	Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. http://znanium.com/catalog.php?bookinfo=474838	
	П.Б. Хорев. Программно-аппаратная защита информации: учебное пособие. М.: Форум, 2009. 352 с. http://www.znanium.com/bookread.php?book=16934	

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

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

Таблица 9 – Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

URL адрес	Наименование
	Не предусмотрено

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.1. Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование
1	Операционная система MS Windows 8 и выше
2	Среда разработки MS Visual Studio 2013 и выше
3	Пакет MS Office 2010 и выше
4	Среда MatLab 7 и выше
5	MicroCap 8 и выше

8.2. Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Состав материально-технической базы представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Компьютерный класс	

10. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

10.1. Состав фонда оценочных средств приведен в таблице 13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных средств
Дифференцированный зачёт	Список вопросов.

10.2. Перечень компетенций, относящихся к дисциплине, и этапы их формирования в процессе освоения образовательной программы приведены в таблице 14.

Таблица 14 – Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер семестра	Этапы формирования компетенций по дисциплинам/практикам в процессе освоения ОП
ОПК-1	«способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики,

математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач»	
1	Математика. Аналитическая геометрия и линейная алгебра
1	Математика. Математический анализ
2	Математика. Аналитическая геометрия и линейная алгебра
2	Математика. Математический анализ
2	Физика
3	Математика. Теория вероятностей и математическая статистика
3	Основы электротехники и радиоэлектроники
3	Физика
4	Основы электротехники и радиоэлектроники
4	Прикладная математика
5	Математические основы обработки информации
5	Мультимедиа технологии
5	Технологии обработки аудио- и видеоданных
6	Программно-аппаратная защита информации
6	Системы и сети передачи данных
6	Теория кодирования
7	Специальные информационные технологии в правоохранительной деятельности
8	Организационная защита информации
ПК-1 «способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз»	
4	Криминалистика
6	Программно-аппаратная защита информации
6	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности (эксплуатационная)
6	Теория информационной безопасности
6	Теория кодирования
7	Методология защиты информации
8	Организационная защита информации
8	Правовая защита информации
8	Технологии защиты от скрытой передачи данных
ПК-2 «способность применять технические и программно-аппаратные средства обработки и защиты информации»	
2	Основы программирования

3	Основы программирования
3	Средства вычислительной техники
5	Криптографическая защита информации
5	Микропроцессорные системы
5	Организация ЭВМ и вычислительных систем
5	Основы электро-, радиоизмерений
6	Криптографическая защита информации
6	Программно-аппаратная защита информации
6	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности (эксплуатационная)
6	Системы и сети передачи данных
6	Теория информационной безопасности
7	Безопасность сетей ЭВМ
7	Защита компьютерных сетей
7	Методология защиты информации
7	Техническая защита информации
8	Защита от вредоносных программ
8	Правовая защита информации
ПК-5 «способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного населения»	
3	Основы электротехники и радиоэлектроники
3	Средства вычислительной техники
4	Основы электротехники и радиоэлектроники
4	Программирование. Методы и технологии программирования
5	Микропроцессорные системы
5	Организация ЭВМ и вычислительных систем
5	Основы электро-, радиоизмерений
6	Программно-аппаратная защита информации
6	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности (эксплуатационная)
6	Системы и сети передачи данных
7	Безопасность сетей ЭВМ
7	Защита компьютерных сетей
8	Программирование. Языки программирования
8	Противодействие преступлениям в сфере информационных технологий
9	Комплексные системы защиты информации в правоохранительной сфере

ПК-6 «способность осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации»	
3	Средства вычислительной техники
6	Программно-аппаратная защита информации
7	Распределенные информационные системы
7	Техническая защита информации
9	Комплексные системы защиты информации в правоохранительной сфере

10.3. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала модульно–рейтинговой системы университета. В таблице 15 представлена 100–балльная и 4–балльная шкалы для оценки сформированности компетенций.

Таблица 15 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100-балльная шкала	4-балльная шкала	
$85 \leq K \leq 100$	«отлично» «зачтено»	<ul style="list-style-type: none"> - обучающийся глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
$70 \leq K \leq 84$	«хорошо» «зачтено»	<ul style="list-style-type: none"> - обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
$55 \leq K \leq 69$	«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> - обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
$K \leq 54$	«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> - обучающийся не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

10.4. Типовые контрольные задания или иные материалы:

1. Вопросы (задачи) для экзамена (таблица 16)

Таблица 16 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
	Учебным планом не предусмотрено

2. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 17)

Таблица 17 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
1	Свойства информации
2	Понятие объекта защиты информации.
3	Понятие информационного процесса
4	Понятие информационной системы
5	Понятие информационного ресурса
6	Организация доступа к ресурсам
7	Основные требования, предъявляемые к системе защиты от копирования.
8	Методы, затрудняющие считывание скопированной информации.
9	Общий алгоритм механизма защиты от несанкционированного использования программ в «чужой» среде размещения.
10	Примеры статических и динамических методов для снятия защиты от копирования.
11	Сравнительный анализ основных методов защиты от копирования.
12	Методы противодействия дизассемблированию
13	Сущность метода, основанного на использовании самогенерируемых кодов
14	Методы защиты программ от исследования.
15	Понятие ядра безопасности
16	Схема классификации вирусов.
17	Проблемы создания высокоэффективной защиты от НСД
18	Сравнительный анализ программных и аппаратных комплексов, рассчитанных на защиту персональных ЭВМ от несанкционированного доступа к ЭВМ, которые разграничивают доступ к информации и устройствам ПЭВМ.
19	Поддержка целостности и доступность информации
20	Методы контроля целостности информации
21	Операционные системы, частично контролируемые компьютерными системами
22	Устройства для работы со смарт-картами
23	Основные преимущества и недостатки системы Crypton Sigma.
24	Мероприятия по защите информации.
25	Мероприятия для защиты информации при ее утечке через сеть электропитания
26	Системы защиты ПЭВМ от несанкционированного доступа к информации.
27	Основные методы защиты от копирования.
28	Метод “водяных знаков”
29	Методы “отпечатков пальцев”.
30	Изучение и обратное проектирование ПО.
31	Задачи защиты от изучения и способы их решения.
32	Методы противодействия дизассемблированию.
33	Аппаратные и программно-аппаратные средства криптозащиты данных.

34	Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования.
35	Защита алгоритма шифрования.
36	Аппаратные средства защиты в РКІ-решениях.
37	Хранения ключевой информации в РКІ-решениях.
38	Требования к системе управления токенами.
39	Комплексная система на базе единого персонального средства аутентификации и хранения ключевой информации.

3. Темы и задание для выполнения курсовой работы / выполнения курсового проекта (таблица 18)

Таблица 18 – Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта

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

4. Вопросы для проведения промежуточной аттестации при тестировании (таблица 19)

Таблица 19 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
	Не предусмотрено

5. Контрольные и практические задачи / задания по дисциплине (таблица 20)

Таблица 20 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	Не предусмотрено

10.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и / или опыта деятельности, характеризующих этапы формирования компетенций, содержатся в Положениях «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».

11. Методические указания для обучающихся по освоению дисциплины

Целью дисциплины является – ознакомление студентов с современными программно-аппаратными средствами защиты информации, овладение методами решения профессиональных задач.

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 обучающимся 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. Введение

Раздел 2. Программно-аппаратные средства реализации идентификации и аутентификации

Тема 2.1. Схемы идентификации и аутентификации.

Тема 2.2. Биометрической идентификация и аутентификация пользователя.

Раздел 3. Программно-аппаратные средства реализации ограничения доступа

Тема 3.1. Система разграничения доступа к информации в компьютерной системе.

Тема 3.2. Средства и методы ограничения доступа к файлам

Тема 3.3. Методы и средства ограничения доступа к компонентам ЭВМ

Раздел 4. Программно-аппаратные средства конфиденциальности, хранения информации

Тема 4.1. Программно-аппаратные средства шифрования.

Тема 4.2. Инфраструктура открытых ключей (PKI).

Тема 4.3. Централизованная система управления средствами аутентификации и хранения ключевой информации пользователей.

Раздел 5. Средства защиты программ

Тема 5.1. Защита программ от несанкционированного копирования

Тема 5.2. Защита программных средств от исследования.

Методические указания для обучающихся по прохождению 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 у обучающегося:

- приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;

- закрепление, развитие и детализация теоретических знаний, полученных на лекциях;
- получение новой информации по изучаемой дисциплине;
- приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

Вариант задания по каждой лабораторной работе обучающийся получает в соответствии с номером в списке группы. Перед проведением лабораторной работы обучающемуся следует внимательно ознакомиться с методическими указаниями по ее выполнению, а также с содержанием соответствующего лекционного курса, при необходимости – изучить самостоятельно дополнительную литературу. В соответствии с заданием обучающийся должен подготовить необходимые данные, выполнить задание лабораторной работы, получить требуемые результаты, оформить и защитить отчет по лабораторной работе.

Структура и форма отчета о лабораторной работе

Отчет о лабораторной работе должен включать в себя: титульный лист, формулировку задания, теоретические положения, используемые при выполнении лабораторной работы, описание процесса выполнения лабораторной работы, полученные результаты и выводы.

Требования к оформлению отчета о лабораторной работе

По каждой лабораторной работе выполняется отдельный отчет. Титульный лист оформляется в соответствии с шаблоном (образцом) приведенным на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации». Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями, приведенными на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации»

Методические указания к выполнению лабораторных работ:

1. Шифр [004.056.5 А 76 004] Аппаратно-программные средства защиты информации: методические указания к выполнению лабораторных работ №1-7/ С.-Петербург. 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. Шифр [004.3 А 76 004] Аппаратные средства вычислительной техники: методические указания к выполнению лабораторных работ №1-8/С.-Петербург. 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.

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.

Примерные темы для самостоятельного изучения:

- Оценка защищенности.
- Локальная и удаленная идентификация.
- Способы хранения идентифицирующей информации.
- Особенности защиты данных от изменения.
- Надежность средств защиты компонент.
- Архитектура платы.

Методические указания для обучающихся по прохождению промежуточной аттестации

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

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