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. Бегаев
(инициалы, фамилия)

(подпись)

«26» мая 2022 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Программно-аппаратные средства защиты информации»
(Наименование дисциплины)

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

Санкт-Петербург– 2022

Лист согласования рабочей программы дисциплины

Программу составил (а)

доц.,к.т.н.,доц.	26.05.22	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.	26.05.22	С.В. Бегаев
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Ответственный за ОП ВО 10.05.03(05)

доц.,к.т.н.,доц.	26.05.22	В.А. Мыльников
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №3 по методической работе

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

Аннотация

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

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ОПК-2 «Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности»

ОПК-9 «Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации»

Содержание дисциплины охватывает круг вопросов, связанных с правовыми и программно-техническими проблемами защиты информации государственных и негосударственных организаций и учреждений, осуществляющих взаимодействие и обмен данными посредством электронных коммуникаций.

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

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

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа.

Язык обучения по дисциплине «русский »

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью дисциплины является приобретение студентами знаний, навыков и умений, связанных с правовыми и программно-техническими проблемами защиты информации государственных и негосударственных организаций и учреждений, осуществляющих взаимодействие и обмен данными посредством электронных коммуникаций.

Основными задачами дисциплины являются:

- ознакомить будущих специалистов с проблемными вопросами, решаемыми в области защиты компьютерной информации
- показать роль современных программно-аппаратных средств защиты информации в обеспечении ее целостности конфиденциальности и доступности
- показать необходимость усвоения знаний о методах и средствах защиты компьютерной информации
- осветить круг вопросов касающихся персональной ответственности должностных лиц за обеспечение безопасности информации, обрабатываемой в современных компьютерных системах
- создать условия для качественного овладения студентами теоретическими знаниями и практическими навыками при решении типовых задач по обеспечению безопасности информационных технологий
- подготовить студентов для самостоятельного использования полученных знаний для правильного выбора решений при применении комплексных систем защиты компьютерной 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 достижения компетенции
Общепрофессиональные компетенции	ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.З.1 знать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности ОПК-2.У.1 уметь выбирать современные информационные технологии и программные средства, в том числе отечественного производства для решения задач профессиональной деятельности ОПК-2.В.1 владеть навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
Общепрофессиональные компетенции	ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития	ОПК-9.З.1 знать технические и программные средства информационной безопасности, основы сетевых технологий и направления их совершенствования ОПК-9.У.1 уметь использовать современные технические, математические и программные средства для решения профессиональных задач

	информационных технологий, средств технической защиты информации, сетей и систем передачи информации	

2. Место дисциплины в структуре ОП

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

– «Информатика»,
– «Языки программирования»,

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

– «Управление информационной безопасностью»,
– «Проектирование безопасных информационных систем»

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
		№6
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	4/ 144	4/ 144
Из них часов практической подготовки		
Аудиторные занятия, всего час.	68	68
в том числе:		
лекции (Л), (час)	34	34
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	34	34
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)	54	54
Самостоятельная работа, всего (час)	22	22
***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 6					
Раздел 1. Программно-аппаратные средства разграничения доступа к компьютерной информации	8		8		4
Раздел 2. Программно-аппаратные средства криптографической защиты информации.	8		8		4
Раздел 3. Программно-аппаратные средства защиты программного обеспечения от копирования и изучения	8		8		6
Раздел 4. Программно-аппаратная защита компьютерной информации от разрушающих программных воздействий	10		10		8
Итого в семестре:	34		34		22
Итого	34	0	34	0	22

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. Введение. Программно-аппаратные средства разграничения доступа к компьютерной информации.* Введение. Цели и задачи дисциплины. Основные понятия и определения в области защиты компьютерной информации. Современная ситуация в области защиты компьютерной информации. Основы защиты компьютерной информации от несанкционированного доступа. Основные термины и определения в области защиты компьютерной информации от НСД. Основные принципы и направления защиты от НСД. Формальные модели управления доступом. Понятие идентификации и аутентификации субъекта. Алгоритмы аутентификации пользователей. Секретная информация, используемая для контроля доступа: ключи и пароли. Злоумышленник и ключи. Классификация средств хранения ключей и идентифицирующей информации. Магнитные диски прямого доступа. Магнитные и интеллектуальные. Средство TouchMemory.
2	*Тема 2. Программно-аппаратные средства криптографической защиты информации.* Роль и место криптографических методов и средств в обеспечении безопасности компьютерной информации. Основные понятия и процедуры технологии управления криптографическими ключами. Аппаратные и программно-аппаратные средства криптозащиты данных. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа. Необходимые и достаточные функции аппаратного средства криптозащиты. Секретная информация, используемая для контроля доступа: ключи и пароли.

3	*Тема 3. Программно-аппаратные средства защиты программного обеспечения от копирования и изучения.* Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования. Разновидности задач защиты от копирования. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО. Привязка программ к гибким магнитным дискам (ГМД). Привязка программ к жестким магнитным дискам (ЖМД). Особенности привязки к ЖМД. Виды меток на ЖМД. Привязка к прочим компонентам штатного оборудования ПЭВМ. Привязка к внешним (добавляемым) элементам ПЭВМ. Привязка к портовым ключам. Использование дополнительных плат расширения. Методы "водяных знаков" и методы "отпечатков пальцев". Понятие изучения и обратного проектирования ПО. Цели и задачи изучения работы ПО. Способы изучения ПО: статическое и динамическое изучение. Роль программной и аппаратной среды. Временная надежность (невозможность обеспечения гарантированной надежности). Защита от отладки. Динамическое преобразование кода. Принцип ловушек и избыточного кода. Защита от дизассемблирования. Принцип внешней загрузки файлов. Динамическая модификация программы. Защита от трассировки по прерываниям.
4	*Тема 4 Программно-аппаратная защита компьютерной информации от разрушающих программных воздействий. Заключение.* Защита от разрушающих программных воздействий. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды. Программные средства антивирусной защиты: основные характеристики, принципы построения и применения.

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 6				
1	Сравнительный анализ понятийных аппаратов различных источников в области защиты информации».	8		1
2	Исследование особенностей криптографической защиты информации при применении классических шифров замены	8		2
3	Защита CD или DVD дисков от копирования с помощью программного средства WildCDProtector	8		3
4	Проверка потенциальных мест записи вредоносного программного обеспечения в системном реестре операционной системы Windows	10		4
	Всего	34		

4.5. Курсовое проектирование/ выполнение курсовой работы

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 6, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	10	10
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	6	6
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	6	6
Всего:	22	22

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)
004.065	Фуфаев Э.В. Базы данных: учебное пособие Э.- М: Академия, 2008.	60
004.6(075)	Галанина В.А. Базы данных: введение в теорию реляционных баз данных. – СПБ:ГОУ ВПО «СПБГУАП»,2008	64
004.4(075)Ф 96	Пакеты прикладных программ: учебное пособие для учреждений СПО/ Э. В. Фуфаев, Л. И. Фуфаева. - 4-е изд., стер.. - М.: Академия, 2008. - 352 с	60
	http://e.lanbook.com/books/element.php?pl1_id=5117 Беленькая, М.Н. Администрирование в информационных системах. [Электронный ресурс] : учебное пособие / М.Н. Беленькая, С.Т. Малиновский, Н.В. Яковенко. — Электрон. дан. — М. : Горячая линия-Телеком, 2011. — 400 с.	
004.65 Д44	Диго, С.М. Базы данных: проектирование и использование: учебник.-М.: Финансы и статистика,2005.	10
681.518(075) П 33	Пирогов В.Ю. Информационные системы и базы данных: организация и проектирование. – СПб:БХВ –Петербург,2009.	15
	http://e.lanbook.com/books/element.php?pl1_id=2713 Зинченко, Л.А. Бионические информационные системы и их практические применения [Электронный ресурс] : / Л.А. Зинченко, В.М. Курейчика, В.Г. Редько. — Электрон. дан. — М. : Физматлит, 2011. — 286 с.	
004.007(075) М 69	Архитектура вычислительных систем: учебное пособие/ В. Г. Хорошевский. - 2-е изд., перераб. и доп.. - М.: Изд-во МГТУ им. Н. Э. Баумана, 2008.	10

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.intuit.ru	Национальный открытый университет ИНТУИТ
http://citforum.ru/security/articles/	Информационная безопасность - статьи, обзоры, книги
http://www.intuit.ru/studies/courses/3499/741/info	Технопарк Mail.ru Group: Базы данных

8. Перечень информационных технологий

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

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование

	Не предусмотрено

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине
Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база

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

Таблица 12 – Состав материально-технической базы

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

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средствдля проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Экзамен	Список вопросов к экзамену; Экзаменационные билеты; Задачи; Тесты.

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

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	– обучающийся глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«хорошо» «зачтено»	– обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	– обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений.

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
1	1. Основные понятия и определения1 в области защиты компьютерной информации. 2. Современная ситуация в области защиты компьютерной информации. 3. Требования к системам защиты информации. 4. Понятие угрозы безопасности компьютерной информации. Интервал потенциальной опасности. 5. Классификация угроз безопасности компьютерной информации. 6. Источники, риски и формы атак на информацию. 7. Принципы защиты компьютерной информации 8. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация; 9. Основные подходы к защите данных от НСД (контроль доступа и разграничение доступа, иерархический доступ к файлу). 10. Формальные модели управления доступом. 11. Классификация средств защиты компьютерной информации от НСД	ОПК-2.3.1

2	12. Аутентификация пользователей. Основные алгоритмы (протоколы) аутентификации. 13. Администрирование сетей в аспекте безопасности информации 14. Защита сетевого файлового ресурса, фиксация доступа к файлам. 15. Доступ к данным со стороны процесса, способы фиксации факта доступа.	ОПК-2.У.1
3	16. Надежность систем ограничения доступа; 17. Защита файлов от изменения; 18. Электронная цифровая подпись (ЭЦП); 19. Методы и средства ограничения доступа к компонентам ЭВМ; 20. Программно-аппаратные средства шифрования; 21. Построение аппаратных компонент криптозащиты данных; 22. Защита алгоритма шифрования.	ОПК-2.В.1
4	23. Принцип чувствительной области и принцип главного ключа, 24. Пароли и ключи, организация хранения ключей; 25. Необходимые и достаточные функции аппаратного средства криптозащиты; 26. Защита программ от несанкционированного копирования; 27. Защита программ от изучения;	ОПК-9.З.1
5	28. Защита программ от отладки, защита от дизассемблирования, 29. Защита программ от трассировки по прерываниям; 30. Защита от разрушающих программных воздействий (РПВ); 31. Компьютерные вирусы как особый класс РПВ; 32. Необходимые и достаточные условия недопущения разрушающего воздействия 33. Понятие изолированной программной среды. 34. Общая характеристика и классификация вредоносных программ. 35. Компьютерные вирусы. Классификация компьютерных вирусов. 36. Основы технологии анализа защищенности компьютерных систем управления и обработки информации. 37. Многоуровневая защита корпоративных сетей.	ОПК-9.У.1

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
	ТЕСТ по дисциплине «Программно-аппаратные средства защиты информации» Вариант № 1 Указания: Задания имеют разное количество вариантов ответа, из которых правильными могут быть как один, так и несколько вариантов. В листе ответа проставляются номера правильных ответов. 1. Сколько уровней возможностей нарушителей предоставляемых им штатными средствами КС предусмотрено классификацией в соответствии с РД ГТК (ФСТЭК)? 1. Один. 2. Два. 3. Три. 4. Четыре. 5. Пять. 6. Семь. 2. Схемы разграничения доступа в которых защитные механизмы встраиваются в каждый объект и осуществляют контроль в соответствии со отеками доступа данного объекта называются: 1. «Списковые» схемы (дискреционный доступ). 2. «Мандатные» схемы (мандатный доступ). 3. «Полномочные» схемы (полномочный доступ). 3. Документ «Служба директорий: обзор концепций, моделей и сервисов» относится к: 1. Оценочным стандартам 2. Техническим спецификациям 3. Руководящим документам ФСТЭК 4. В каком году был принят Стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Trusted Computer System Evaliation Criteria, TCSEC)? 1. 1975 2. 1980 3. 1985 4. 1990 5. Каким стандартом было введено понятие: «Сетевая доверенная вычислительная база»? 1. Department of Defense Trusted Computer System Evaliation Criteria, TCSEC	

2. Trusted Network Interpretation
3. ISO/IEC 15408-99
4. ГОСТ/ИСО МЭК 15408:2002
6. Какой стандарт называют «Оранжевой книгой»?
1. Стандарт Министерства обороны США «Критерии оценки доверенных компьютерных
систем» (Department of Defense Trusted Computer System Evaliation Criteria, TCSEC)
2. Гармонизированные критерии Европейских стран" [европейские критерии]
3. Международный стандарт ISO/IEC 15408-99 «Критерии оценки безопасности
информационных технологий» (Evaluation criteria for IT security)
1. Какой стандарт сокращенно называют «Общими критериями» (ОК)?
1. Стандарт Министерства обороны США «Критерии оценки доверенных компьютерных
систем»
2. Международный стандарт ISO/IEC 15408-99
3. Британский стандарт BS 7799 «Управление информационной безопасностью.
Практические правила»
4. Какое из перечисленных понятий было введено в Стандарте Министерства обороны США
«Критерии оценки доверенных компьютерных систем» (Trusted Computer System
Evaliation Criteria, TCSEC)?
1. Сервисы безопасности
2. Политика безопасности
3. Оценочные уровни доверия - ОУД
4. Международный стандарта ISO/IEC 15408-99 раскрывает (описывает):
1. Систематический подход к вопросам доступности, формирование архитектурных принципов ее обеспечения.
2. Различие между системами и продуктами информационных технологий, но для унификации требований вводится единое понятие - объект оценки
3. Критерии оценки безопасности информационных технологий
5. Как называется документ, в котором в целях добровольного многократного
использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг?
1. Технические условия
2. Спецификация
3. Регламент
4. Стандарт
6. Цель создания политики информационной безопасности?

	1. Для организационно-технической поддержки политики формирования и использования информационных ресурсов при осуществлении доступа к информации 2. Для защиты от внешних деструктивных воздействий 3. Для защиты от недобросовестных работников (пользователей) 7. Совокупность принципов, правил и рекомендаций, определяющих порядок организации защиты информации, обрабатываемой в конкретной компьютерной системе, зафиксированная документально называется: 1. Технической политикой безопасности компьютерной системы 2. Политикой информационной безопасности компьютерной системы 3. Стандарт безопасности компьютерной системы 8. Формулировка целей, которые преследует организация в области безопасности информации, определение общих направлений в достижении этих целей является составной частью: 1. Политики безопасности верхнего (правового и административного) уровня 2. Политики безопасности среднего (процедурного) уровня 3. Политики безопасности нижнего (программно-аппаратного) уровня 4. Нет правильного ответа 9. Контроль участников взаимодействия является ключевым моментом при составлении политики информационной безопасности: 1. Политики безопасности верхнего (правового и административного) уровня 2. Политики безопасности среднего (процедурного) уровня 3. Политики безопасности нижнего (программно-аппаратного) уровня 4. Нет правильного ответа 10. Список подчиненных политик безопасности является основой: 1. Acceptable use policies - AUP 2. Корневой политики безопасности 3. Политики формирования и использования информационных ресурсов 11. Совокупность требований и правил по информационной безопасности для объекта информационной безопасности, выработанных в соответствии с требованиями руководящих и нормативных документов в целях противодействия заданному множеству угроз информационной безопасности, с учетом ценности защищаемой информационной сферы и стоимости системы обеспечения информационной безопасности называется: 1. Стандарт безопасности 2. Политика информационной безопасности 3. Политика безопасности верхнего уровня 4. Корневая политика безопасности	

	12. В каком документе (разделе) политики безопасности отражается ответ на вопрос: «Существуют ли ограничения на установку ПО»? 1. Сертификате безопасности 2. Acceptable use policies - AUPS 3. Incident response plan - IRP 4. Password policy 13. Какой документ включает в себя следующие подразделы: политику формирования и использования информационных ресурсов, политику информационной безопасности и техническую политику? 1. Стандарт безопасности 2. Техническая спецификация 3. Информационная политика 4. Политика информационной безопасности 5. Политика использования информационных ресурсов 14. В политике безопасности какого уровня описывается отношение к передовым, но еще недостаточно проверенным технологиям защиты информации? 1. Правового и административного 2. Процедурного 3. Аппаратно-программного 15. Что определяет системная информационная политика? 1. Принципы, порядок и правила интеграции информационных ресурсов 2. Принципы, порядок и правила построения систем защиты информации 3. Принципы, порядок и правила разграничения доступа к информационным ресурсам 16. Как называется внешняя или внутренняя по отношению к атакуемой компьютерной системе программа, обладающая определенными деструктивными функциями по отношению к этой системе? 1. Компьютерный вирус 2. Программная закладка 3. Аппаратная закладка 17. Как называется несаморазмножающаяся программа, обеспечивающая злоумышленнику возможности несанкционированного доступа к защищаемой информации? 1. Компьютерный вирус 2. Ловушка 3. Люк 4. Логическая бомба 18. Какая из перечисленных функций не относится к программных закладкам? 1. Уничтожение информации 2. Самостоятельное распространение в компьютерных системах 3. Перехват и передача информации 4. Целенаправленная модификация кода программы 19. По какому признаку классифицируются «драйверные закладки»?	

	1. По методу внедрения 2. По принципу действия 3. По деструктивным последствиям 20. Какое из перечисленных воздействий не относится к моделям воздействия программных закладок? 1. Уборка мусора 2. Искажение 3. Наблюдение 4. Копирование 5. Перехват 21. К какому виду РПС относится «Клавиатурный шпион» 1. К программным закладкам 2. К вирусам 3. К бактериям 22. Какие из перечисленных свойств присущи компьютерным вирусам? 1. Способность к включению своего кода в тела других файлов и системных областей памяти компьютера 2. Способность к последующему самостоятельному выполнению и самовоспроизведению 3. Способность к самостоятельному распространению в КС 4. Все перечисленные свойства 5. Только 1 и 3 свойство 6. Только 2 и 3 свойство 23. Сотрудник Лехайского университета (США) Фред Коэн: 1. Впервые создал антивирус 2. Сделал сообщение о возможности существования компьютерных вирусов 3. Является создателем вируса-червя 24. В чем принципиальное отличие компьютерного вируса от программной закладки? 1. Сложностью написания 2. Возможностью деструктивного воздействия 3. Способностью к саморазмножению и модификации 4. Всеми вышеперечисленными свойствами 25. Как называются закладки, интерфейс которых, совпадает с интерфейсом некоторых служебных программ, требующих ввод конфиденциальной информации 1. Прикладные закладки 2. Исполняемые закладки 3. Закладки-имитаторы 4. Закладки-невидимки 26. По какому признаку вирус классифицируется как резидентный вирус? 1. По режиму функционирования 2. По объекту внедрения 3. По особенностям реализуемого алгоритма	

	4. По деструктивным возможностям 27. По какому признаку вирус классифицируется как «stealth-вирус»? 1. По объекту внедрения 2. По особенностям реализуемого алгоритма 3. По деструктивным возможностям 28. По какому признаку вирус классифицируется как «загрузочный (бутовый) вирус»? 1. По объекту внедрения 2. По особенностям реализуемого алгоритма 3. По режиму функционирования 29. Вирусы, содержащие в себе алгоритмы шифрования и обеспечивающие различие разных копий вируса называются: 1. Вирусы-спутники 2. Stealth-вирусы 3. MtE-вирусы 4. Репликаторы 30. К какому типу компьютерных вирусов относятся полиморфные вирусы? 1. К MtE-вирусам 2. К Stealth-вирусам 3. К вирусам-спутникам 31. По какому признаку компьютерный вирус классифицируется как репликатор? 1. По особенностям реализуемого алгоритма 2. По объекту внедрения 3. По наличию дополнительных возможностей 32. Вирусы, создающие для заражаемых файлов одноименные файлы с кодом вируса и переименовывающие исходные файлы называются: 1. Вирусы - спутники 2. Вирусы - невидимки 3. Вирусы - мутанты 33. Как называется компьютерный вирус, который использует слабую защищенность некоторых ОС и заменяет некоторые их компоненты (драйверы дисков, прерывания)? 1. Файловым 2. Загрузочным 3. Stealth-вирус 4. Репликатор 34. Как называются группы из нескольких вирусов? 1. Поливирусами 2. Семейством вирусов 3. Вирусным классом 4. Нет верных ответов 35. Какие вирусы характеризуются способностью самостоятельно	

передавать свой код на
удаленный сервер или рабочую станцию?
1. Файловые вирусы
2. Бутовые (загрузочные) вирусы
3. Нет правильных ответов
4. Файловых и загрузочных вирусы

ВАРИАНТ № 2

Указания:
Задания имеют один правильный вариант ответа. В листе ответа проставляются
номера правильных ответов.

1. Сколько классов АВС определено РД ГТК «Средства антивирусной защиты. Показатели защищенности и требования по защите от вирусов»
1. три
2. пять
3. семь
4. девять
5. нет правильных ответов

2. Деятельность, направленную на предотвращение получения защищаемой информации
заинтересованным субъектом с нарушением установленных правовыми документами или
собственником (владельцем информации) прав или правил доступа к защищаемой
информации называется:
1. Обеспечение целостности информации
2. Обеспечение доступности информации
3. Защита информации от НСД
4. Защита информации

2. Как называется тип документа, в котором в целях добровольного многократного
использования устанавливаются порядок осуществления процессов производства,
эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или
оказания услуг?
1. Регламент
2. Стандарт
3. Спецификация
4. Сертификат

7. Как называется Спецификация X.509
1. «Служба директорий: каркасы сертификатов открытых ключей и атрибутов».
2. «Служба директорий: обзор концепций, моделей и сервисов».
3. «Архитектура безопасности для взаимодействия открытых систем».

8. Что обозначает аббревиатура ФСТЭК?

1. Федеральная система технологического и эксплуатационного контроля.
2. Федеральная служба технического и экспортного контроля.
3. Федеральная служба технического и экспертного контроля.
4. Федеральная служба таможенного и экспертного контроля.
5. Нет правильного ответа.
9. Как называется процесс присвоение объектам и субъектам доступа идентификатора и
(или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов?
1. Аутентификация.
2. Национализация.
3. Идентификация.
4. Паролизация.
10. Для каких целей при администрировании, парольной системы, устанавливается
ограничение числа попыток ввода пароля?
1. Усложняет задачу злоумышленника при попытке подобрать пароль по словарю
2. Препятствует интерактивному подбору паролей злоумышленником
3. Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального
опробования».
4. Защищает от неправомерных действий системного администратора, имеющего доступ к
паролю в момент создания учетной записи.
5. Для всех целей перечисленных в пунктах 1-4.
11. Какой из перечисленных методов не применяется для аутентификации пользователей?
1. Системы, основанные на знании некоторой секретной информации.
2. Системы, основанные на владении некоторым специальным предметом или устройством.
3. Системы, основанные на биометрических характеристиках.
4. Нет правильного ответа. Все применяются.
12. Может ли на одном компьютере создаваться несколько учетных записей с правами
администратора?
1. Нет, только должна быть только одна учетная запись данного типа.
2. Может быть не менее одной учетной записи данного типа.
3. Допускается не более двух учетных записей данного типа.
4. Нет правильных ответов.
13. Свойство информации, заключающееся в ее актуальности и непротиворечивости, ее
защищенности от разрушения и несанкционированного изменения называется:
1. Доступностью.
2. Целостностью.

	3. Конфиденциальностью. 14. Какой из перечисленных сервисов не является сервисом безопасности? 1. Экранирование. 2. Туннелирование. 3. Архивирование. 4. Шифрование. 5. Контроль целостности. 6. Контроль защищенности. 15. По какому критерию классифицируется удаленная атака, приводящая к искажению информации? 1. По цели воздействия 2. По характеру воздействия 3. По расположению субъекта атаки относительно атакуемого объекта 16. Какой классификационный признак позволяет судить о так называемой «степени удаленности» атаки? 1. По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие 2. По расположению субъекта атаки относительно атакуемого объекта 3. По условию начала осуществления воздействия 17. Какая из перечисленных удаленных атак является пассивной? 1. DNS spoofing 2. SYN flooding 3. Sniffing 4. Перехват пакетов на маршрутизаторе 18. Что означает аббревиатура NIDS: 1. Международная Организация по Стандартизации 2. Системы обнаружения (выявления) атак 3. Лавинное затопление ICMP-пакетами 19. Преимуществом метода данного типа является возможность обнаружения новых атак без необходимости постоянного изменения параметров функционирования модуля. О каком методе идет речь? 1. Сигнатурном (signature) 2. Шаблонном (pattern) 3. На основе обнаружения злоупотреблений 4. Нет правильных ответов 20. Принцип работы этого метода заключается в обнаружении несоответствия между текущим режимом функционирования КС и моделью штатного режима работы, заложенной в параметрах метода. О каком методе обнаружения атак идет речь? 1. На основе обнаружения аномального поведения (поведенческие методы)	

	2. На основе обнаружения злоупотреблений 3. Сигнатурный (signature) 4. Нет правильных ответов 21. Как называются СОА обнаруживающие атаки, направленные на всю сеть или сегмент? 1. host-based 2. network-based 3. Системы обнаружения атак на уровне хоста 4. Нет правильных ответов 22. Недостатком таких систем является то, что они сильно загружают процессор и требуют больших объемов дискового пространства для хранения журналов регистрации. О каких типах СОА идет речь? 1. network-based 2. host-based 3. Системы обнаружения атак уровня сети 4. Нет правильных ответов 23. Что означает аббревиатура DoS? 1. атаки типа «отказ в обслуживании» 2. атаки типа «затопление» 3. атаки типа «подмена адреса» 4. нет правильных ответов 24. Если атакующая программа, запущенная на сетевом компьютере, ждет посылки от потенциальной цели атаки определенного типа запроса, который будет условием начала осуществления атаки, то такая атака классифицируется как: 1. Атака по запросу от атакуемого объекта 2. Атака по наступлению определенного события на атакуемом объекте 3. Безусловная атака 25. Межсетевой экран предназначен: 1. Для защиты программ от несанкционированного копирования 2. Для обеспечения безопасного доступа к внешней сети и ограничения доступа внешних пользователей к внутренней сети. 3. Для защиты экрана монитора от несанкционированного снятия информации с помощью технических средств разведки. 4. Нет правильных ответов. 26. Какой из перечисленных компонентов не входит в состав технологии Межсетевого экранирования (МЭ): 1. Сетевая политика безопасности. 2. Централизованное управление. 3. Политика применения антивирусных средств при работе в сети.	

4. Подсистема сбора статистики и предупреждения об атаке.
5. Все перечисленные компоненты входят в технологию МЭ.
27. Политика доступа к сетевым сервисам является подчиненной политикой:
1. Политики сетевой безопасности
2. Усиленной аутентификации
3. Политики реализации межсетевых экранов
4. Нет правильных ответов
28. Чем определяются правила доступа к ресурсам внутренней сети, при реализации политики межсетевого экранирования?
1. Политикой реализации межсетевых экранов
2. Политикой доступа к сетевым сервисам
3. Нет правильных ответов
29. Чем определяется список сервисов Internet, к которым пользователи должны иметь
ограниченный доступ?
1. Политикой доступа к сетевым сервисам
2. Политикой реализации межсетевых экранов
3. Нет правильных ответов
30. Возможность некоторых МЭ по блокированию (уничтожению) пакетов, попадающих на
МЭ, по заданному критерию на основе данных, содержащихся в заголовках пакетов и
текущих параметров окружающей среды называется:
1. Фильтрация с применением Посредника (транспортного) уровня соединения (circuit-level
proxy)
2. Простая фильтрация пакетов (с помощью фильтрующего маршрутизатора)
3. Фильтрация с применением Посредника прикладного уровня (application proxy)
4. Нет правильных ответов
31. Какие из перечисленных пунктов определяют достоинства простой фильтрации пакетов?
1. Локальная сеть может быть сделана невидимой из глобальной сети
2. Способность гибкого регулирования (ограничения) пропускной способности
3. Использование политики «запрещено все, что не разрешено»
4. Нет правильных ответов
32. Какие из перечисленных пунктов определяют достоинства шлюза прикладного уровня
(application proxy)?
1. «Прозрачность» связи
2. Гибкость в определении правил фильтрации
3. Небольшая задержка при прохождении пакетов
4. Нет правильных ответов

	33. Какие из перечисленных пунктов определяют недостатки фильтрующего маршрутизатора (простой фильтрации пакетов) 1. Не учитывается состояние соединения транспортного и прикладного уровней 2. При нарушении работоспособности МЭ все компьютеры за ним становятся полностью незащищенными либо недоступными 3. Не учитывается содержимое IP-пакетов 4. Все пункты определяют недостатки простой фильтрации пакетов 5. Нет правильных ответов 34. Функция МЭ, скрывающая внутренние адреса объектов (субъектов) от внешних субъектов называется: 1. Экранирование 2. Трансляция адреса 3. Правило фильтрации 4. Нет правильных ответов 35. Как называется наука о создании и анализе систем безопасной связи? 1. Криптология 2. Криптография 3. Криптоанализ 36. Как называется дисциплина (раздел науки), охватывающая принципы, средства и методы преобразования данных для сокрытия их информационного содержимого? 1. Криптоанализ 2. Криптография 3. Криптология 37. Как называется конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных? 1. Шифр 2. Ключ 3. Криптоалгоритм 38. Как называется совокупность обратимых преобразований множества возможных открытых данных (текстов) на множество возможных зашифрованных данных (криптограмм), осуществляемых по определенным правилам? 1. Шифр 2. Ключ 3. Криптоалгоритм__	

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. Программно-аппаратные средства разграничения доступа к компьютерной информации
Раздел 2. Программно-аппаратные средства криптографической защиты информации.
Раздел 3. Программно-аппаратные средства защиты программного обеспечения от копирования и изучения
Раздел 4. Программно-аппаратная защита компьютерной информации от разрушающих программных воздействий

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 (ЛР)

- В задании должно быть четко сформулирована задача, выполняемая в ЛР;
- Описаны входные и выходные данные для проведения ЛР;
- ЛР должна выполняться на основе полученных теоретических знаниях;
- Выполнение ЛР должно осуществляться на основе методических указаний, предоставляемых преподавателем;
- ЛР должна выполняться в специализированном компьютерном классе и может быть доработана студентом в домашних условиях, если позволяет ПО;
- Итогом выполненной ЛР является отчет.

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

- Лабораторная работа (ЛР) предоставляется в печатном/или электронном виде;
- ЛР должна соответствовать структуре и форме отчета представленной выше;
- ЛР должна 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.

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 являются:

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

11.2. Методические указания для обучающихся по прохождению промежуточной аттестации.

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

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

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

– дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой