

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

Кафедра № 33

УТВЕРЖДАЮ

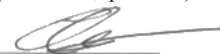
Руководитель направления

проф., д.т.н., доц.

(должность, уч. степень, звание)

С.В. Беззатеев

(инициалы, фамилия)



(подпись)

«26» мая 2022 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита в операционных системах»

(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– 2022

Лист согласования рабочей программы дисциплины

Программу составил (а)

доц.,к.т.н.,доц.

(должность, уч. степень, звание)



26.05.22

(подпись, дата)

В.А. Мыльников

(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«27» мая 2021 г, протокол № 10

Заведующий кафедрой № 33

д.т.н.,доц.

(уч. степень, звание)



26.05.22

(подпись, дата)

С.В. Беззатеев

(инициалы, фамилия)

Ответственный за ОП ВО 10.03.01(01)

доц.,к.т.н.,доц.

(должность, уч. степень, звание)



26.05.22

(подпись, дата)

В.А. Мыльников

(инициалы, фамилия)

Заместитель директора института №3 по методической работе

(должность, уч. степень, звание)



26.05.22

(подпись, дата)

Н.В. Решетникова

(инициалы, фамилия)

Аннотация

Дисциплина «Защита в операционных системах» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 10.03.01 «Информационная безопасность» направленности «Безопасность компьютерных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

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

ОПК-1.1 «Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах»

ОПК-1.2 «Способен администрировать средства защиты информации в компьютерных системах и сетях»

ОПК-1.4 «Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями»

Содержание дисциплины охватывает круг вопросов, связанных с изучением терминологии, понятийного аппарата и общих подходов к обеспечению информационной безопасности операционных систем; изучением средств и методов управления доступом в защищенных операционных системах; изучением средств и методов аутентификации пользователей в защищенных операционных системах; изучением средств и методов реализации аудита в защищенных операционных системах; изучением средств и методов интеграции защищенных операционных систем в защищенную сеть.

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

Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц, 180 часов.

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью изучения дисциплины является теоретическая и практическая подготовка специалистов к деятельности, связанной с применением защищенных операционных систем, а также средств и методов обеспечения защиты информации в операционных системах.

Задачи дисциплины:

–изучение терминологии, понятийного аппарата и общих подходов к обеспечению информационной безопасности операционных систем;

–изучение средств и методов управления доступом в защищенных операционных системах;

–изучение средств и методов аутентификации пользователей в защищенных операционных системах;

–изучение средств и методов реализации аудита в защищенных операционных системах;

изучение средств и методов интеграции защищенных операционных систем в защищенную сеть.

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 информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.3.1 знает классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей; назначение, функции и обобщенную структуру операционных систем; назначение и основные компоненты систем баз данных
Общепрофессиональные компетенции по направленности	ОПК-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	ОПК-1.1.3.1 знает архитектуру и принципы построения и защиты операционных систем ОПК-1.1.3.2 знает программные интерфейсы настроек политик управления доступом в операционных системах ОПК-1.1.У.1 умеет использовать

		средства защиты информации операционных систем для противодействия угрозам безопасности информации ОПК-1.1.В.1 владеет навыками настройки антивирусной защиты в соответствии с действующими требованиями
Общепрофессиональные компетенции по направленности	ОПК-1.2 Способен администрировать средства защиты информации в компьютерных системах и сетях	ОПК-1.2.3.2 знает принципы функционирования программных средств криптографической защиты информации ОПК-1.2.В.2 владеет навыками установки программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации
Общепрофессиональные компетенции по направленности	ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	ОПК-1.4.3.3 знает принципы функционирования программных средств криптографической защиты информации

2. Место дисциплины в структуре ОП

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

- «Основы информационной безопасности»,
- «Программно-аппаратные средства защиты информации»

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

- «Разработка и эксплуатация автоматизированных систем в защищенном исполнении»,
- «Защита информации в распределенных информационных системах»,
- «Управление информационной безопасностью».

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	№8
1	2	3	4
Общая трудоемкость дисциплины, ЗЕ/ (час)	5/ 180	2/ 72	3/ 108

Из них часов практической подготовки			
Аудиторные занятия, всего час.	91	51	40
в том числе:			
лекции (Л), (час)	54	34	20
практические/семинарские занятия (ПЗ), (час)			
лабораторные работы (ЛР), (час)	37	17	20
курсовой проект (работа) (КП, КР), (час)			
экзамен, (час)	27		27
Самостоятельная работа, всего (час)	62	21	41
Вид промежуточной аттестации: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Дифф. Зач., Экз.	Дифф. Зач.	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. Понятие защищенной операционной системы	14		4		6
Раздел 2. Управление доступом	20		13		15
Итого в семестре:	34		17		21
Семестр 8					
Раздел 3. Идентификация, аутентификация и авторизация	10		10		20
Раздел 4. Интеграция защищенных операционных систем в защищенную сеть	10		10		21
Итого в семестре:	20		20		41
Итого	54	0	37	0	62

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	<u>Понятие защищенной операционной системы</u> Общая характеристика ОС; назначение и возможности систем семейства UNIX, систем семейства Windows. Интерфейс взаимодействия ОС с пользователями. Общие принципы управления ресурсами вычислительных систем. Понятия процесса (потока) в ОС. Средства межпроцессорного взаимодействия. Управление памятью в ОС. Виртуальная память. Обработка прерываний от устройств ввода-вывода в ОС. Структурная обработка исключений.

	<p>Синхронный и асинхронный ввод-вывод.</p> <p>Угрозы безопасности операционной системы, классификация угроз, наиболее распространенные угрозы. Понятие защищенной операционной системы. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты.</p>
2	<p><u>Управление доступом</u></p> <p>Субъекты, объекты, методы и права доступа, привилегии субъекта доступа. Требования к правилам управления доступом. Дискреционное управление доступом. Матрица доступа. Изолированная программная среда. Мандатное управление доступом. Метки доступа. Контроль информационных потоков. Проблемы реализации мандатного управления доступом в операционных системах.</p> <p>Управление доступом в операционных системах семейства UNIX. Субъекты, объекты, методы и права доступа. UID, EUID, GID, EGID. Атрибуты защиты объектов доступа. Средства динамического изменения полномочий субъектов: SUID/SGID. Расширения стандартной системы управления доступом в Linux.</p> <p>Управление доступом в операционных системах семейства Windows. Субъекты, объекты, методы и права доступа, привилегии субъекта. Маркеры доступа субъектов, дескрипторы защиты объектов. Порядок проверки прав доступа, порядок назначения дескрипторов защиты создаваемым объектам. Средства динамического изменения полномочий субъектов: олицетворение субъектов доступа. Расширения дискреционной системы управления доступом: автоматическое наследование атрибутов защиты объектов, ограниченные маркеры доступа, мандатный контроль целостности, контроль учетных записей, элементы изолированной программной среды</p>
3	<p><u>Идентификация, аутентификация и авторизация</u></p> <p>Понятия идентификации, аутентификации и авторизации пользователей. Средства и методы хранения эталонных копий аутентификационной информации. Протоколы передачи аутентификационной информации по каналам вычислительной сети. Криптографическое обеспечение аутентификации пользователей.</p> <p>Аутентификация на основе паролей. Средства и методы защиты от компрометации и подбора паролей. Парольная аутентификация в Linux, библиотеки PAM. Парольная аутентификация в Windows, средства управления параметрами аутентификации.</p> <p>Аутентификация на основе внешних носителей ключа. Особенности проверки аутентификационной информации для различных типов носителей ключа. Проблемы генерации, рассылки и смены ключей.</p> <p>Биометрическая аутентификация: общая схема, преимущества, проблемы. Достоинства и недостатки различных схем биометрической аутентификации.</p>
4	<p><u>Интеграция защищенных операционных систем в защищенную сеть</u></p> <p>Преимущества доменной архитектуры локальной сети. Понятие домена, контроллер домена. Порядок наделения пользователей домена полномочиями на отдельных компьютерах. Централизованное управление политикой безопасности в домене.</p> <p>«Лесная» доменная архитектура Windows 2000/2003/2008/2010.</p> <p>Идентификация компьютеров в сети. Двусторонние транзитивные отношения доверия. Средства и методы синхронизации баз данных контроллеров разных доменов одного леса. Аутентификация по Kerberos. Групповая политика. Делегирование полномочий</p>

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	Анализ операционных систем	2		1
2	Изучение характеристик операционных систем	2		1
3	Основные атрибуты доступа	2		2
4	Управление доступом в Linux	2		2
5	Реализация локального доступа в Linux	2		2
6	Реализация сетевого доступа в Linux	2		2
7	Управление доступом в Windows	2		2
8	Реализация локального доступа в Windows	2		2
9	Реализация сетевого доступа в Windows	1		2
Семестр 8				
1	Средства аутентификации операционных систем	2		3
2	Управление средствами аутентификации в Linux	2		3
3	Управление средствами аутентификации в Windows	2		3
4	Изучение системы PAM и организация контроллера домена, протокола LDAP	2		3
5	Документирование политики безопасности	2		4
6	Централизованное планирование политики безопасности в лесу доменов Windows	2		4
7	Централизованное планирование политики безопасности в Linux	2		4
8	Настройки протокола KERBEROS, NTLM	2		4
9	Настройки протокола SMB	4		4
Всего		37		

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	Семестр 8, час
1	2	3	4
Изучение теоретического материала дисциплины (ТО)		11	21
Курсовое проектирование (КП, КР)			
Расчетно-графические задания (РГЗ)			
Выполнение реферата (Р)			
Подготовка к текущему контролю успеваемости (ТКУ)		5	10
Домашнее задание (ДЗ)			
Контрольные работы заочников (КРЗ)			
Подготовка к промежуточной аттестации (ПА)		5	10
Всего:	62	21	41

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)
004.056 Б 40	Безопасность операционных систем : методические указания к выполнению лабораторных работ / С.-Петерб. гос. ун-т аэрокосм. приборостроения ; сост. В. А. Мыльников. - Санкт-Петербург : Изд-во ГУАП, 2020. - 53 с. : табл. - Библиогр.: с. 52 (4 назв.). - Б. ц. - Текст : непосредственный.	5
004 Б 28	Батаев, А. В. Операционные системы и среды : учебник [для СПО] / А. В. Батаев, Н. Ю. Налютин, С. В. Сеницын. - 4-е изд., стер. - Москва : Академия, 2020. - 272 с. : рис., табл. - (Профессиональное образование). - Библиогр.: с. 267 (19 назв.). - ISBN 978-5-4468-8681-4 : 1240.25 р. - Текст : непосредственный. Имеет гриф Федерального институт развития образования	20
004.4 К 17	Калужный, Виталий Павлович (доц.). Операционные системы [Текст] : учебное пособие / В. П. Калужный, К. В. Зац ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2012. - 145 с.	68

658 О-60	Операционные системы для организации производства в промышленности [Текст] : учебное пособие / Н. В. Артамонова [и др.] ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2012. - 224 с.	100
004.4 Т 18	Таненбаум, Э. Современные операционные системы [Текст] = Modern operating systems / Э. Таненбаум. - 3-е изд. - СПб. : ПИТЕР, 2015. - 1120 с.	40
004 А 76	Аппаратные средства поддержки операционных систем [Текст] : методическое пособие / С.-Петерб. гос. ун-т аэрокосм. приборостроения ; сост. Н. В. Кучин. - СПб. : Изд-во ГУАП, 2015. - 43 с.	86

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

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

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

URL адрес	Наименование
www.intuit.ru	Национальный Открытый Университет "ИНТУИТ"

8. Перечень информационных технологий

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

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

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

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база

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

Таблица 12 – Состав материально-технической базы

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

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средств для 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.
Дифференцированный зачёт	Список вопросов; Тесты; Задачи.

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»	<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.
«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.
«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.
«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.

10.3. 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	Определение и назначение ОС Виды ОС Функции ОС Архитектура операционной системы Структура ОС Монолитная архитектура Микроядерная архитектура	ОПК-2.3.1
2	Понятия вычислительного процесса и ресурса Прерывания Системные вызовы Процесс, поток. Создание процессов и потоков Состояния потока Планирование и диспетчеризация потоков Алгоритмы планирования Управление памятью Типы адресов	ОПК-1.1.3.1
3	Методы распределения памяти без использования дискового пространства Методы распределения памяти с использованием дискового пространства	ОПК-1.1.3.2
4	Понятие виртуальной памяти Страничное распределение виртуальной памяти Сегментное распределение виртуальной памяти Странично-сегментное распределение виртуальной памяти Свопинг	ОПК-1.1.У.1
5	Назначение и функции файловой системы Логическая организация файловой системы Файловая система FAT Файловая система NTFS Контроль доступа к файлам Основные понятия безопасности ОС	ОПК-1.1.В.1
6	Системный подход к обеспечению безопасности Симметричные криптосистемы Асимметричные криптосистемы Аутентификация Аутентификация на основе многофакторных паролей Аутентификация на основе одноразовых паролей	ОПК-1.2.3.2
7	Цифровые сертификаты Цифровые подписи Авторизация доступа	ОПК-1.2.В.2
8	Аудит Средства администрирования ОС Windows Server Средства безопасности ОС Windows Server	ОПК-1.4.3.3

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
1	Субъекты, объекты, методы, права и привилегии Linux и Windows	ОПК-2.3.1

2	Дискреционное управление доступом в современных операционных системах	ОПК-1.1.3.1
3	Средства защиты от вредоносного программного обеспечения в современных операционных системах	ОПК-1.1.3.2
4	Проблемы реализации мандатного управления доступом в современных операционных системах	ОПК-1.1.У.1
5	Управление доступом в Linux	ОПК-1.1.В.1
6	Базовые средства управления доступом в Windows: маркеры доступа, дескрипторы защиты.	ОПК-1.2.3.2
7	Управление средствами аутентификации в Linux. Управление доменами Windows	ОПК-1.2.В.2
8	Назначение атрибутов защиты вновь создаваемым объектам Windows, наследование дескрипторов защиты	ОПК-1.4.3.3

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

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

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

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

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
1	<p>1. Пользователь, (потребитель) информации – это ... *пользователь, использующий совокупность программно-технических средств *субъект, пользующийся информацией, в соответствии с регламентом доступа *владелец фирмы или предприятия *фирма – разработчик программного продукта, которая занимается ее дистрибуцией</p> <p>2. Право доступа к информации – это ... *совокупность правил доступа к информации, установленных правовыми документами или собственником либо владельцем информации *лицо или процесс, осуществляющие несанкционированного доступа к информации *возможность доступа к информации, не нарушающая установленные правила разграничения доступа *совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям *нарушение установленных правил разграничения доступа</p> <p>3. Под целостностью информации понимается ... *защита от несанкционированного доступа к информации *актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения *возможность за приемлемое время получить требуемую информационную услугу</p> <p>4. Информация может быть защищена от ... *пересылки ее по электронной почте *психологического состояния *санкционированных пользователей *утечки побочных электромагнитных излучений *физического лица *несанкционированного доступа</p> <p>5. К видам информации с ограниченным доступом относится ... *коммерческая тайна *государственная тайна *общественные данные *банковская тайна *персональные данные *личная тайна</p> <p>6. Утилиты скрытого управления позволяют ... запускать операционную</p>	ОПК-2.3.1

	<p>систему разрушать жесткий диск запускать и уничтожать файлы выводить сообщения стирать информацию</p> <p>7. К правовым мерам компьютерной безопасности можно отнести ... *соответствие гражданскому законодательству *нормы ответственности сотрудников *защиту авторских прав *организацию обслуживания объекта *защиту от несанкционированного доступа к системе</p> <p>8. К организационным мерам компьютерной безопасности можно отнести ... *организацию обслуживания объекта *защиту от хищений, диверсий и саботажа *охрану объекта *план восстановления работоспособности объекта *тщательный подбор персонала *установку оборудования сигнализации</p> <p>9. Сертификат продукта, обеспечивающий информационную безопасность, ... *подтверждает его соответствие стандарту РФ *подтверждает отсутствие в продукте незадекларированных возможностей *просто является документом, необходимым для реализации продукции *подтверждает его качество</p> <p>10. К правовым мерам компьютерной безопасности можно отнести ... *тщательный подбор персонала *соответствие уголовному законодательству *защиту авторских прав * резервирование важных подсистем</p>	
2	<p>11. Политика доступа к информации – это ... *совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям *нарушение установленных правил разграничения доступа *совокупность правил доступа к информации, установленных правовыми документами или собственником либо владельцем информации *лицо или процесс, осуществляющие несанкционированного доступа к информации *доступ к информации, не нарушающий установленные правила разграничения доступа (эти правила служат для регламентации права доступа к компонентам системы)</p> <p>12. К техническим мерам компьютерной безопасности можно отнести ... резервное копирование резервирование важных подсистем идентификацию и аутентификацию обнаружение утечек воды оборудование систем пожаротушения установку оборудования сигнализации</p> <p>13. В стандартной политике безопасности установка программных продуктов непосредственно пользователем корпоративной рабочей станции ... *Запрещена *разрешена *разрешена, за исключением компьютерных игр *разрешена, но только с устного согласия сотрудника ИТ-отдела</p> <p>14. Под конфиденциальностью информации понимается ... *защита от несанкционированного доступа к информации *актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения *возможность за приемлемое время получить требуемую информационную услугу</p> <p>15. Неверно, что к видам вредоносного программного обеспечения относится ... *руткит (Rootkit) *отладчик *компьютерные вирусы *анализатор сетевого трафика (снифер) *программы удаленного управления (если отсутствует функция скрытого внедрения)</p> <p>16. Неверно, что к основным целям аудита ИБ относится ... *регламентация действий пользователя *локализация потенциально опасных мест *оценка уровня защищенности ИБ *разработка рекомендаций по повышению уровня безопасности</p> <p>17. Расставьте этапы аудита ИБ в их логическом порядке: 1 локализация потенциально опасных мест ИБ 2 разработка рекомендаций по повышению уровня безопасности ИБ 3 составление и анализ списка рисков 4 оценка уровня защищенности ИБ</p> <p>18. ... – помещенная на компьютер пользователя без его согласия,</p>	ОПК-1.1.3.1

	<p>контроля и уведомления средство слежения</p> <p>19. Основной смысл разграничения прав доступа пользователей – ... *обеспечение безопасности информации внутри компании и возможности ее использования лишь непосредственно владельцем/исполнителем *ущемление работодателем гражданских прав работника *создание трудностей для сотрудников компании, с последующем увольнением неугодных компании людей</p> <p>20. Анализ рисков включает в себя ... *выявление существующих рисков и оценку их величины *анализ причинения ущерба и величины ущерба, наносимого ресурсам ИС, в случае осуществления угрозы безопасности *мероприятия по обследованию безопасности ИС, с целью определения того какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите *набор адекватных контрмер осуществляется в ходе управления рисками</p>	
3	<p>21. Программное обеспечение, которое не должно быть доступно в нормальной работе пользователя, – ... *системные утилиты и системные редакторы *средства защиты *средства разработки, утилиты *средства защиты, системные утилиты</p> <p>22. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) ... *влечет только наложение административного штрафа *влечет уголовную ответственность и наложение административного штрафа *влечет во всех случаях уголовную ответственность *не влечет за собой уголовной ответственности</p> <p>23. Под локальной безопасностью информационной системы подразумевается ... *запрет использования посторонних информационных продуктов, обновление антивирусных баз *установка минимальной оперативной памяти и маленького монитора для невозможности осуществления пользователем взлома системы *ограничение пользователя на локальном рабочем месте от других сотрудников с помощью перегородок</p> <p>24. Система защиты информации – это ... *разработка стратегии защиты бизнеса компаний *область информационных технологий *комплексная совокупность программно-технических средств, обеспечивающая защиту информации *совокупность органов и/или исполнителей, используемая ими техника защиты информации</p> <p>25. Идентификация субъекта – это ... *проверка подлинности субъекта с данным идентификатором *установление того, является ли субъект именно тем, кем он себя объявил *процедура предоставления законному субъекту соответствующих полномочий и доступных ресурсов системы *процедура распознавания субъекта по его идентификатору *установление лиц или процессов, осуществляющих несанкционированного доступа к информации</p> <p>26. К техническим мерам компьютерной безопасности можно отнести ... *резервное электропитание *защиту от несанкционированного доступа к системе *установку замков *резервное копирование данных *защиту от несанкционированного копирования *защиту от хищений, диверсий и саботажа</p> <p>27. Авторизация субъекта – это ... *процедура предоставления законному субъекту соответствующих полномочий и доступных ресурсов системы *установление лиц или процессов, осуществляющих несанкционированного доступа к информации *установление того, является ли субъект именно тем, кем он себя объявил *проверка подлинности субъекта с данным идентификатором *процедура распознавания субъекта по его идентификатору</p> <p>28. Сервисом безопасности, используемым в распределенных системах и</p>	ОПК-1.1.3.2

	<p>сетях является ... *авторизация *разграничение доступа *экранирование и туннелирование *маршрутизация *аутентификация *идентификация</p> <p>29. К организационным мерам компьютерной безопасности можно отнести ... *организацию обслуживания объекта *ведение особо важных работ несколькими сотрудниками *резервное электропитание *защиту от несанкционированного доступа к системе *тщательный подбор персонала *выбор места расположения объекта</p> <p>30. Отличительная способность компьютерных вирусов от вредоносного *повысить привилегии в системе *собирать информацию *к самовоспроизведению *уничтожать информацию</p>	
4	<p>31. С точки зрения законодательства (права) существует уровень доступа к информации ... *закрытый доступ *открытый доступ *ограниченный доступ *интеллектуальная собственность *без ограничения права доступа *наносающий вред при распространении</p> <p>32. В системное программное обеспечение входят: *языки программирования *операционные системы *компьютерные игры *графические редакторы *текстовые редакторы</p> <p>33. Неверно, что к биометрическим данным относится ... *проекция лица *тембр голоса *серия паспорта *отпечатки пальцев *адрес прописки</p> <p>34. Операционная система цифровой вычислительной системы предназначена для: *обеспечения совмещения различных интерфейсов *обеспечения удобной работы пользователя *обеспечения определенного уровня эффективности цифровой вычислительной системы за счет автоматизированного управления ее работой и предоставляемого пользователям набора услуг.</p> <p>35. К основным разновидностям вредоносного воздействия на систему относится ... *иницирование ложных действий *модификация выполняемых функций *удаление системы *копирование данных из системы *создание помех в работе *вывод из строя</p> <p>36. Информация – это ... *совокупность знаний, накопленная человечеством *совокупность рефлексий между идеей и материей на макро- и микроуровнях *сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления *совокупность принципов, методов и форм управления</p> <p>37. Аппаратные и программные средства и технологии гарантировать абсолютную надежность и безопасность данных в компьютерных системах ... *не могут *могут только для государственных организаций *могут *могут только для коммерческих компаний *могут только для частных лиц</p> <p>38. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются ... *организацией, в которой работает гражданин *законом либо другими нормативными актами, служебной запиской, а также организацией, в которой работает гражданин *служебной запиской *законом либо другими нормативными актами</p> <p>39. Вирусные программы принято делить по ... *степени ценности *особенности алгоритма вируса *среде обитания вируса *способу заражения *общим признакам</p> <p>40. По видам различают антивирусные программы ... *вакцины *ревизоры *доктора *сканеры *принтеры *сторожа</p>	ОПК-1.1.У.1
5	<p>41. К направлениям, в которых осуществляется защита информации встроенными методами прикладных программ относится ... *симметричных криптографических преобразований *криптографическое закрытие *разграничение доступа к данным *борьба с макровирусами *аудита</p> <p>42. Европейские критерии безопасности ITSEC устанавливают ... классов безопасности 5 8 10 7 15 12</p> <p>43. К основным видам систем обнаружения вторжений относятся ...</p>	ОПК-1.1.В.1

	<p>*локальные *межсетевые *активные *синхронные *пассивные</p> <p>44. Под доступностью информации понимается ... *возможность за приемлемое время получить требуемую информационную услугу *защита от несанкционированного доступа к информации *актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения</p> <p>45. Вирусные программы принято делить по ... возможности осуществления следящим признакам особенности алгоритма вируса направленности деструктивным возможностям</p> <p>46. В соответствии с законодательством ответственность за незаконное ограничение доступа к информации и за нарушение режима защиты информации несут ... служащие органов государственной власти администраторы информационных систем служащие охранных агентств руководители</p> <p>47. По существующим правилам разрабатывать, производить защиты информации может только предприятие, имеющее ... аккредитацию начальный капитал лицензию сертификат</p> <p>48. Несанкционированный доступ к информации – это ... *лицо или процесс, осуществляющие несанкционированного доступа к информации. *совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям *нарушение установленных правил разграничения доступа *доступ к информации, не нарушающий установленные правила разграничения доступа. Правила разграничения доступа служат для регламентации права доступа к компонентам системы *совокупность правил доступа к информации, установленных правовыми документами или собственником либо владельцем информации</p> <p>49. Деятельностью по сертификации шифровальных средств на территории РФ занимается ... ФСБ ФСТЭК ФСО МВД ФСВТС</p> <p>50. Современную организацию ЭВМ предложил: Норберт Винер Чарльз Беббидж Джон фон Нейман</p>	
6	<p>51. В «Концепции защиты СВТ и АС от НСД к информации» как главные средства защиты от несанкционированного доступа к информации рассматриваются ... *компьютерные и коммуникационные системы *системы разграничения доступа *инфраструктуры промышленных предприятий *биометрические системы</p> <p>52. Неверно, что к модулям антивируса относится ... *сканер файлов по сигнатурам *средство обновления программных модулей и баз сигнатур *модуль перехвата нажатия клавиш *монитор (перехватчик и анализатор запускаемых процессов)</p> <p>53. Основные средства проникновения вирусов в компьютер ... копирование файлов компьютерные сети съемные диски игровые программы</p> <p>54. Под физической безопасностью информационной системы подразумевается ... *ограничение физического доступа к системе по средствам пропусков, паролей, биометрических данных *запрет физического входа и выхода из здания компании в период с 10 до 18 часов ограничение *подключения к информационной системе «из вне»</p> <p>55. На компьютерах применяются локальные политики безопасности ... *параметров безопасности *симметричных криптографических преобразований *прав пользователей *подстановки *гаммирования *аудита</p> <p>56. В состав европейских критериев ITSEC по информационной безопасности входит ... цели безопасности конфиденциальность информации закрытость информации целостность информации защищенность от проникновения спецификация функций безопасности</p> <p>57. К видам информации с ограниченным доступом относится ... профессиональная тайна государственная тайна персональные данные</p>	ОПК-1.2.3.2

	<p>служебная тайна общественные данные промышленная тайна</p> <p>58. Утилиты скрытого управления позволяют ... перезагружать компьютер запускать и уничтожать файлы принимать и отправлять файлы переименовывать файлы и их расширения вводить новую информацию</p> <p>59. В состав европейских критериев ITSEC по информационной безопасности входит ... описание механизмов безопасности доступность информации конфиденциальность информации защищенность от воздействий полнота информации цели безопасности</p> <p>60. Установка лицензионного ПО является ... обязательным критерием информационной безопасности бесполезной тратой корпоративных денежных средств необязательным критерием информационной безопасности</p>	
7	<p>61. Санкционированный доступ к информации – это ... *доступ к информации, не нарушающий установленные правила разграничения доступа *совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям *лицо или процесс, осуществляющие несанкционированного доступа к информации *нарушение установленных правил разграничения доступа *совокупность правил доступа к информации, установленных правовыми документами или собственником либо владельцем информации</p> <p>62. Информационная безопасность, по законодательству РФ, – это ... *методологический подход к обеспечению безопасности *маркетинг *состояние защищенности национальных интересов РФ в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства *свод норм, соблюдение которых призвано защитить компьютеры и сеть от несанкционированного доступа *состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства</p> <p>63. Аутентификация субъекта – это ... *процедура распознавания субъекта по его идентификатору *проверка подлинности субъекта с данным идентификатором *установление того, является ли субъект именно тем, кем он себя объявил *процедура предоставления законному субъекту соответствующих полномочий и доступных ресурсов системы *установление лиц или процессов, осуществляющих несанкционированного доступа к информации</p> <p>64. Аудит информационной безопасности – это... *оценка текущего состояния системы информационной безопасности *проверка используемых компанией информационных систем, систем безопасности *это проверка способности успешно противостоять угрозам *специальная проверка соответствия организации и эффективности защиты информации *установленным требованиям и/или нормам</p> <p>65. Программы keylogger используются для ... *удаления вирусов *сбора информации, вводимой с клавиатуры *удаления программ-шпионов *контроля за состоянием центрального процессора</p> <p>66. Отличительная особенность компьютерных вирусов по сравнению с другим вредоносным программным обеспечением – их способность ... *к самовоспроизведению *уничтожать информацию *собирать информацию *повысить привилегии в системе</p> <p>67. В европейских критериях безопасности ITSEC установлено ... классов безопасности 5 7 8 10 12 15</p> <p>68. Неверно, что защита информации встроенными методами прикладных программ может осуществляется в направлении ... *аудита *борьбы с макровирусами *криптографического закрытия *разграничения доступа к данным</p> <p>69. Неверно, что к источникам угроз информационной безопасности относятся ... *человеческий фактор *правовые аспекты</p>	ОПК-1.2.В.2

<p>функционирования ис *стихийные бедствия *аппаратные сбои *ошибки проектирования и разработки ис</p> <p>70. Неверно, что к сервисам безопасности, используемым в распределенных системах и сетях, относится ... *идентификация *аутентификация *маршрутизация *разграничение доступа *экранирование и туннелирование</p> <p>71. Неверно, что к основным видам систем обнаружения вторжений относятся ... системы *сетевые *локальные *межсетевые</p>	
--	--

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 изучения дисциплины «Безопасность операционных систем» является теоретическая и практическая подготовка специалистов к деятельности, связанной с применением защищенных операционных систем, а также средств и методов обеспечения защиты информации в операционных системах.

Задачи дисциплины:

- изучение терминологии, понятийного аппарата и общих подходов к обеспечению информационной безопасности операционных систем;
 - изучение средств и методов управления доступом в защищенных операционных системах;
 - изучение средств и методов аутентификации пользователей в защищенных операционных системах;
 - изучение средств и методов реализации аудита в защищенных операционных системах;
- изучение средств и методов интеграции защищенных операционных систем в защищенную сеть.

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;
- научится методически обрабатывать материал (выделять главные мысли и положения, приходиться 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:

- Тема № 1. Понятие защищенной операционной системы
- Тема № 2. Управление доступом
- Тема № 3. Идентификация, аутентификация и авторизация
- Тема № 4. Интеграция защищенных операционных систем в защищенную сеть

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

Задания для лабораторных работ заключаются в решении задач, рассмотренных в ходе лекций, таких как:

- Управление доступом в Linux
- Управление доступом в Windows
- Анализ операционных систем
- Средства аутентификации операционных систем
- Управление средствами аутентификации в Linux
- Управление средствами аутентификации в Windows
- Документирование политики безопасности
- Централизованное планирование политики безопасности в лесу доменов Windows
- Централизованное планирование политики безопасности в Linux

Лабораторные занятия проводятся после чтения лекций, дающих теоретические основы для их выполнения. Допускается выполнение лабораторных занятий до прочтения лекций с целью облегчения изучения теоретического материала при наличии описаний работ, включающих необходимые теоретические сведения или ссылки на конкретные учебные издания, содержащие эти сведения.

Преподаватель имеет право определять содержание лабораторных работ, выбирать методы и средства проведения лабораторных исследований, наиболее полно отвечающие их особенностям и обеспечивающие высокое качество учебного процесса.

Преподаватель формирует рубежные и итоговые результаты (рейтинги) студента по результатам выполнения лабораторных работ.

На лабораторном занятии студент имеет право задавать преподавателю и (или) лаборанту вопросы по содержанию и методике выполнения работы и требовать ответа по существу обращения.

Студент имеет право на выполнение лабораторной работы по оригинальной методике с согласия преподавателя и под его надзором – при безусловном соблюдении требований безопасности.

К выполнению лабораторной работы допускаются студенты, подтвердившие готовность в объеме требований, содержащихся в методических указаниях к лабораторной работе и (или) в устных предварительных указаниях преподавателя.

В ходе лабораторных занятий студенты ведут необходимые записи, составляют (по требованию преподавателя) итоговый письменный отчет. На первом занятии цикла лабораторных работ преподаватель должен дать конкретные указания по составлению и оформлению отчетов с целью обеспечения единообразия. В зависимости от особенностей цикла лабораторных занятий отчет составляется каждым студентом индивидуально, либо общий отчет – подгруппой из 2-3 студентов. По окончании лабораторной работы студенты обязаны представить отчет преподавателю для проверки с последующей защитой. По согласованию с преподавателем допускается представление к защите отчета о лабораторной работе во время следующего лабораторного занятия или в индивидуальные сроки, оговоренные с преподавателем. Допускается по согласованию с преподавателем представлять отчет о лабораторной работе в электронном виде.

Лабораторное занятие состоит из следующих элементов: вводная часть, основная и заключительная.

Вводная часть обеспечивает подготовку студентов к выполнению заданий работы. В ее состав входят:

- формулировка темы, цели и задач занятия, обоснование его значимости в профессиональной подготовке студентов;
- изложение теоретических основ работы;
- характеристика состава и особенностей заданий работы и объяснение методов (способов, приемов) их выполнения;
- характеристика требований к результату работы;
- инструктаж по технике безопасности при эксплуатации технических средств;
- проверка готовности студентов выполнять задания работы;
- указания по самоконтролю результатов выполнения заданий студентами.

Основная часть включает процесс выполнения лабораторной работы, оформление отчета и его защиту. Она может сопровождаться дополнительными разъяснениями по ходу работы, устранением трудностей при ее выполнении, текущим контролем и оценкой результатов отдельных студентов, ответами на вопросы студентов. Возможно пробное выполнение задания(ий) под руководством преподавателя.

Заключительная часть содержит:

- подведение общих итогов занятия;
- оценку результатов работы отдельных студентов;
- ответы на вопросы студентов;
- выдачу рекомендаций по устранению пробелов в системе знаний и умений студентов, по улучшению результатов работы;
- сбор отчетов студентов для проверки, изложение сведений, касающихся подготовки к выполнению следующей работы.

Вводная и заключительная части лабораторного занятия проводятся фронтально. Основная часть может выполняться индивидуально или коллективно (в зависимости от формы организации занятия).

Структура и форма отчета о лабораторной работе

Отчёт по лабораторной работе оформляется индивидуально каждым студентом, выполнившим необходимые (независимо от того, выполнялся ли эксперимент индивидуально или в составе группы студентов). Страницы отчёта следует пронумеровать (титульный лист не нумеруется, далее идет страница 2 и т.д.). Титульный лист отчёта должен содержать фразу: «Отчёт по лабораторной работе «Название работы», чуть ниже: Выполнил студент группы (номер группы) (Фамилия, инициалы)». Внизу листа следует указать текущий год. Например, Отчёт по лабораторной работе № (номер работы) «Введение в спектральный анализ», Выполнил студент группы 5221 Иванов И.И. Вторая страница текста, следующая за титульным листом, должна начинаться с пункта: Цель работы. Отчёт, как правило, должен содержать следующие основные разделы:

1. Цель работы;
2. Теоретическая часть;
3. Программное обеспечение, используемое в работе;
4. Результаты;
5. Выводы.

В случае необходимости в конце отчёта приводится перечень литературы.

Требования к оформлению отчета о лабораторной работе

Теоретическая часть должна содержать минимум необходимых теоретических сведений о предметной области. Не следует копировать целиком или частично методическое пособие (описание) лабораторной работы или разделы учебника.

В разделе Программное обеспечение необходимо описать, с помощью каких инструментальных средств и каким образом были разработаны модели и получены результаты. Рисунки, блок-схемы, описание модели и её особенностей, необходимость отладки – все это должно быть представлено в указанном разделе.

Раздел Результаты включает в себя скриншоты программного приложения, полученные при выполнении лабораторной работы. Рисунки, графики и таблицы нумеруются и подписываются заголовками.

Выводы не должны быть простым перечислением того, что сделано. Здесь важно отметить, какие новые знания о предмете исследования были получены при выполнении работы, к чему привело обсуждение результатов, насколько выполнена заявленная цель работы. Выводы по работе каждый студент делает самостоятельно. В случае необходимости в конце отчёта приводится Список литературы, использованной при подготовке к работе. В тексте отчёта делаются краткие ссылки на литературу (учебники, справочники, иные источники...) номером в квадратных скобках, напр., [1]. Литературные источники нумеруются по мере их появления в тексте отчёта. В конце отчёта даётся их подробный список. На все источники списка литературы должны быть ссылки в тексте отчёта, там, где это необходимо.

При сдаче отчёта преподаватель может сделать устные и письменные замечания, задать дополнительные вопросы. Все ответы на дополнительные вопросы, обсуждения выполняются студентом на отдельных листах, включаемых в отчёт (при этом в тексте основного отчёта делается сноска или другой значок, которому будет соответствовать новый материал). При этом письменные замечания преподавателя должны остаться в тексте для ясности динамики работы над отчётом.

Объём отчёта должен быть оптимальным для понимания того, что и как сделал студент, выполняя работу. Обязательные требования к отчёту включают общую и специальную грамотность изложения, а также аккуратность оформления.

После приёма преподавателем отчёт хранится на кафедре.

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).

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