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)
«25» мая 2023 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Безопасность инфокоммуникационных систем»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.05.05
Наименование направления подготовки/ специальности	Безопасность информационных технологий в правоохранительной сфере
Наименование направленности	Организация и технологии защиты информации (в информационных системах)
Форма обучения	очная

Санкт-Петербург– 2023

Лист согласования рабочей программы дисциплины

Программу составил (а)

доц.,к.т.н.,доц.	25.05.23	В.А. Мыльников
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«25» мая 2023 г, протокол № 10

Заведующий кафедрой № 33

д.т.н.,доц.	25.05.23	С.В. Беззатеев
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Ответственный за ОП ВО 10.05.05(05)

доц.,к.т.н.,доц.	25.05.23	В.А. Мыльников
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №3 по методической работе

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

Аннотация

Дисциплина «Безопасность инфокоммуникационных систем» входит в образовательную программу высшего образования – программу специалитета по направлению подготовки/ специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» направленности «Организация и технологии защиты информации (в информационных системах)». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-2 «Способен проводить контроль работоспособности технических и программно-аппаратных средств обработки и защиты информации»

ПК-3 «Способен осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния»

ПК-8 «Способен анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности»

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.

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 7 зачетных единиц, 252 часа.

Язык обучения по дисциплине «русский »

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью изучения дисциплины «Безопасность инфо-коммуникационных 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.

1.2. Дисциплина входит в состав части, формируемой участниками образовательных отношений, образовательной программы высшего образования (далее – ОП ВО).

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

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Профессиональные компетенции	ПК-2 Способен проводить контроль работоспособности технических и программно-аппаратных средств обработки и защиты информации	ПК-2.З.1 знать технические и программные средства информационной безопасности, основы сетевых технологий и направления их совершенствования
Профессиональные компетенции	ПК-3 Способен осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния	ПК-3.З.2 знать порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях ПК-3.В.1 владеть навыками установки, настройки, администрирования и эксплуатации компонентов систем защиты информации ПК-3.В.2 владеть навыками диагностики и восстановления работоспособности компонентов систем защиты информации
Профессиональные компетенции	ПК-8 Способен анализировать	ПК-8.В.1 владеть навыками использования информационных сервисов для автоматизации

	структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности	прикладных и информационных процессов анализа систем защиты информации

2. Место дисциплины в структуре ОП

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

– «Информатика и информационные технологии в правоохранительной деятельности»,

– «Математическая логика и теория алгоритмов»,

– Дискретная математика

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

– « Комплексные системы защиты информации в правоохранительной сфере»,

– «Технологии защиты от скрытой передачи данных»,

– Производственная преддипломная практика.

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	№7
1	2	3	4
Общая трудоемкость дисциплины, ЗЕ/ (час)	7/ 252	3/ 108	4/ 144
Из них часов практической подготовки	68	34	34
Аудиторные занятия, всего час.	136	68	68
в том числе:			
лекции (Л), (час)	68	34	34
практические/семинарские занятия (ПЗ), (час)			
лабораторные работы (ЛР), (час)	68	34	34
курсовой проект (работа) (КП, КР), (час)			
экзамен, (час)	36		36
Самостоятельная работа, всего (час)	80	40	40
***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 6					
Раздел 1. Понятие защищенной операционной системы	14		8		20
Раздел 2. Управление доступом	20		26		20
Итого в семестре:	34		34		40
Семестр 7					
Раздел 3. Идентификация, аутентификация и авторизация	16		16		20
Раздел 4. Интеграция защищенных операционных систем в защищенную сеть	18		18		20
Итого в семестре:	34		34		40
Итого	68	0	68	0	80

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	Понятие защищенной операционной системы 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. Синхронный и асинхронный ввод-вывод. Угрозы безопасности операционной системы, классификация угроз, наиболее распространенные угрозы. Понятие защищенной операционной системы. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты.
2	Управление доступом 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. 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. Управление доступом в операционных системах семейства Win-

	dows. 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
3	Идентификация, аутентификация и авторизация 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. 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. Аутентификация на основе внешних носителей ключа. Особенности проверки аутентификационной информации для различных типов носителей ключа. Проблемы генерации, рассылки и смены ключей. Биометрическая аутентификация: общая схема, преимущества, проблемы. Достоинства и недостатки различных схем биометрической аутентификации.
4	Интеграция защищенных операционных систем в защищенную сеть Преимущества доменной архитектуры локальной сети. Понятие домена, контроллер домена. Порядок наделения пользователей домена полномочиями на отдельных компьютерах. Централизованное управление политикой безопасности в домене. «Лесная» доменная архитектура Windows 2000/2003/2008/2010. 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

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	Анализ операционных систем	4	2	1
2	Изучение характеристик операционных систем	4	4	1
3	Основные атрибуты доступа	4	4	2
4	Управление доступом в Linux	4	4	2
5	Реализация локального доступа в Linux	4	4	2
6	Реализация сетевого доступа в Linux	4	2	2
7	Управление доступом в Windows	4	2	2
8	Реализация локального доступа в Windows	4	2	2
9	Реализация сетевого доступа в Windows	2	1	2
Семестр 7				
1	Средства аутентификации операционных систем	4	4	3
2	Управление средствами аутентификации в Linux	4	4	3
3	Управление средствами аутентификации в Windows	4	4	3
4	Изучение системы PAM и организация контроллера домена, протокола LDAP	4	4	3
5	Документирование политики безопасности	4	4	4
6	Централизованное планирование политики безопасности в лесу доменов Windows	4	4	4
7	Централизованное планирование политики безопасности в Linux	4	4	4
8	Настройки протокола KERBEROS, NTLM	4	4	4
9	Настройки протокола SMB	2	2	4
	Всего	68	59	

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	Семестр 7, час
1	2	3	4
Изучение теоретического материала дисциплины (ТО)	40	20	20
Курсовое проектирование (КП, КР)			
Расчетно-графические задания (РГЗ)			

Выполнение реферата (Р)			
Подготовка к текущему контролю успеваемости (ТКУ)	20	10	10
Домашнее задание (ДЗ)			
Контрольные работы заочников (КРЗ)			
Подготовка к промежуточной аттестации (ПА)	20	10	10
Всего:	80	40	40

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. Синицын. - 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	Калюжный, Виталий Павлович (доц.). Операционные системы [Текст] : учебное пособие / В. П. Калюжный, 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] :	100

	учебное пособие / Н. В. Артамонова [и др.] ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2012. - 224 с.	
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 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.
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»	– обучающийся глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	– обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления;

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
	– 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	Определение и назначение ОС Виды ОС Функции ОС Архитектура операционной системы Структура ОС Монолитная архитектура Микроядерная архитектура	ПК-2.З.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	ПК-3.З.2
3	Методы распределения памяти без использования дискового пространства Методы распределения памяти с использованием дискового пространства	ПК-3.В.1
4	Понятие виртуальной памяти Страничное распределение виртуальной памяти Сегментное распределение виртуальной памяти Странично-сегментное распределение виртуальной памяти Свопинг Системный подход к обеспечению безопасности Симметричные криптосистемы Асимметричные криптосистемы Аутентификация Аутентификация на основе многоразовых паролей Аутентификация на основе одноразовых паролей	ПК-3.В.2

5	Назначение и функции файловой системы Логическая организация файловой системы Файловая система FAT Файловая система NTFS Контроль доступа к файлам Основные понятия безопасности ОС Цифровые сертификаты Цифровые подписи Авторизация доступа Аудит Средства администрирования ОС Windows Server Средства безопасности ОС Windows Server	ПК-8.В.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
1	Субъекты, объекты, методы, права и привилегии Linux и Windows	ПК-2.З.1
2	Дискреционное управление доступом в современных операционных системах	ПК-3.З.2
3	Средства защиты от вредоносного программного обеспечения в современных операционных системах	ПК-3.В.1
4	Проблемы реализации мандатного управления доступом в современных операционных системах Управление средствами аутентификации в Linux. Управление доменами Windows	ПК-3.В.2
5	Управление доступом в Linux Базовые средства управления доступом в Windows: маркеры доступа, дескрипторы защиты. Назначение атрибутов защиты вновь создаваемым объектам Windows, наследование дескрипторов защиты	ПК-8.В.1

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. 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 дистрибьюцией	

	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 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 4. Информация может быть защищена от ... *пересылки ее по электронной почте *психологического состояния *санкционированных пользователей *утечки побочных электромагнитных излучений *физического лица *несанкционированного доступа 5. К видам информации с ограниченным доступом относится … *коммерческая тайна *государственная тайна *общественные данные *банковская тайна *персональные данные *личная тайна 6. Утилиты скрытого управления позволяют … запускать операционную систему разрушать жесткий диск запускать и уничтожать файлы выводить сообщения стирать информацию 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 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 9. Сертификат продукта, обеспечивающий информационную безопасность, … *подтверждает его соответствие стандарту РФ *подтверждает отсутствие в продукте незадекларированых возможностей *просто является документом, необходимым для реализации продукции *подтверждает его качество 10. К правовым мерам компьютерной безопасности можно отнести … *тщательный подбор персонала *соответствие уголовному законодательству *защиту авторских прав * резервирование важных подсистем	

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 инфо-коммуникационных 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, 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:

– 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