Автономная некоммерческая профессиональная образовательная организация «Калининградский колледж управления»

Лист актуализации рабочей программы дисциплины[1]

ОП.12 «Управление доступом в информационных системах»

Специальность: *09.02.04 - «Информационные системы (по отраслям)»*

В целях актуализации образовательной программы с учетом появления новых учебников, учебных пособий и других учебно-методических материалов в рабочую программу внесены следующие изменения (дополнения):

1. п. 5.2 Лицензионное программное обеспечение - проведена актуализация лицензионного программного обеспечения.

2. п. 6 Оценочные средства и методические материалы по итогам освоения дисциплины внесено дополнение, что при разработке оценочных средств преподавателем используются базы данных педагогических измерительных материалов, предоставленных ООО «Научно-исследовательский институт мониторинга качества образования»

3. п. 8. Дополнительные ресурсы информационно - телекоммуникационной сети «Интернет» необходимые для освоения дисциплины - внесен ресурс https://i-exam.ru/ - Единый портал интернет-тестирования в сфере образования.

4. в Приложение 1 к РПД п. 6.2 (Методические рекомендации и указания) – актуализированы рекомендации по проведению учебных занятий с обучающимися с применением электронного обучения и дистанционных образовательных технологий.

Разработчик: *Воробейкина И. В.* «15» мая 2023 г.
(ФИО, ученая степень, ученое звание) (дата)

Изменения (дополнения) в рабочую программу рассмотрены и утверждены на заседании учебно-методического совета, протокол № 57 от «25» мая 2023 г.

СОГЛАСОВАНО:

Руководитель ОПОП _____ Шульгина Н.В.

Начальник УМУ _____ Усенок С.С.

26 мая 2023 г. М.П.

[1] Лист актуализации сдается в электронном виде в Учебный отдел АНПОО «ККУ»

Автономная некоммерческая профессиональная образовательная организация
«КАЛИНИНГРАДСКИЙ КОЛЛЕДЖ УПРАВЛЕНИЯ»

Утверждено
Учебно-методическим советом Колледжа
протокол заседания
№ 24 от 20 февраля 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
УПРАВЛЕНИЕ ДОСТУПОМ В ИНФОРМАЦИОННЫХ СИСТЕМАХ
(ОП.12)

По специальности	**09.02.04 Информационные системы (по отраслям)**
Квалификация	**Техник по информационным системам**
Форма обучения	**Очная**

Рабочий учебный план по специальности
утвержден директором 05 ноября 2019 г.

Калининград

Лист согласования рабочей программы дисциплины

Рабочая программа дисциплины «Управление доступом в информационных системах» разработана в соответствии с федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.04 Информационные системы (по отраслям), утвержденным приказом Министерства образования и науки Российской Федерации от 14 мая 2015 г. № 525.

Составитель (автор) – старший преподаватель Воробейкина И.В.

Рабочая программа дисциплины рассмотрена и одобрена на заседании Учебно-методического совета колледжа, протокол № 24 от 20 февраля 2020 г.

Регистрационный номер ИС 40/20

1. Цели и задачи освоения дисциплины

Целями освоения дисциплины «Управление доступом в информационных системах» являются:

- профессиональная ориентация студентов с первых дней их обучения по выбранной специальности;
- обучение студентов основам научной организации труда, ознакомление студентов с основными документами специальности, а также правилами поиска и работы с источниками информации;
- формирование у техников цельного представления о безопасности информационных систем как о наборе различных методик и инструментариев защиты информации, их совместного использования в целях повышения уровня конфиденциальности, целостности и доступности информации в автоматизированных информационных системах.

2. Место дисциплины в структуре ППСЗ

Учебная программа дисциплина «Управление доступом в информационных системах» является частью программы подготовки специалистов среднего звена (ППССЗ) по специальности 09.02.04.Информационные системы (по отраслям). Дисциплина относится к общепрофессиональным (ОП 12), вариативная часть.

В процессе освоения дисциплины обучающиеся осваивают навыки работы с программными и аппаратными средствами защиты информации, их совместного использования в целях повышения уровня конфиденциальности, целостности и доступности информации в автоматизированных информационных системах.

Изучение данной дисциплины базируется на содержании знаний полученных по следующим учебным дисциплинам: Информационные технологии, Операционные системы, Устройство и функционирование информационной системы, Основы алгоритмизации и программирования, Компьютерные сети.

В свою очередь освоение материала дисциплины «Управление доступом в информационных системах» обеспечивает преемственность знаний в дальнейшем процессе обучения при освоении следующих дисциплин: Эксплуатация средств автоматизации, Технические средства автоматизации, Основы информационного менеджмента, Экспертные системы, Правовое обеспечение профессиональной деятельности, а также всех видов практики.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

В результате изучения дисциплины «Управление доступом в информационных системах» обучающийся должен:

иметь практический опыт:

- инсталляции, настройки и сопровождения одной из информационных систем;
- выполнения регламентов по обновлению, техническому сопровождению и восстановлению данных информационной системы;
- сохранения и восстановления базы данных информационной системы;
- организации доступа пользователей к информационной системе в рамках компетенции конкретного пользователя;
- участия в экспериментальном тестировании информационной системы на этапе опытной эксплуатации и нахождения ошибок кодирования в разрабатываемых модулях информационной системы;
- участия в оценке качества и экономической эффективности информационной системы;
- модификации отдельных модулей информационной системы;

уметь:

- осуществлять сопровождение информационной системы, настройку под конкретного пользователя, согласно технической документации;
- поддерживать документацию в актуальном состоянии;
- идентифицировать технические проблемы, возникающие в процессе эксплуатации системы;
- производить документирование на этапе сопровождения;
- организовывать разноуровневый доступ пользователей информационной системы в рамках своей компетенции;
- строить архитектурную схему организации;
- осуществлять выбор модели построения информационной системы и программных средств;

знать:

- основные задачи сопровождения информационной системы;
- отказы системы;
- восстановление информации в информационной системе;
- принципы организации разноуровневого доступа в информационных системах, политику безопасности в современных информационных системах.

В процессе изучения дисциплины «Управление доступом в информационных системах» у обучающихся формируются следующие общие компетенции:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

В процессе изучения дисциплины «Управление доступом в информационных системах» у обучающихся формируются следующие профессиональные компетенции:

ПК 1.1. Собирать данные для анализа использования и функционирования информационной системы, участвовать в составлении отчетной документации, принимать участие в разработке проектной документации на модификацию информационной системы.

ПК 1.5. Разрабатывать фрагменты документации по эксплуатации информационной системы и фрагменты методики обучения пользователей.

4. Объем, структура и содержание дисциплины с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся.

4.1 Объем дисциплины

Объем дисциплины	Всего акад. часов для очной формы обучения
Всего академических часов учебных занятий	108
В том числе:	
контактная работа обучающихся с преподавателем (по видам учебных занятий):	72
Лекции	24
Семинары, практические занятия	30
Практикумы	-
Лабораторные работы	18
Самостоятельная работа обучающихся:	26
Подготовка к контрольным работам (семинарам)	-

Выполнение творческих заданий (задач, рефератов)	-
Курсовое проектирование	-
Консультации	6
Промежуточной аттестации обучающегося - экзамен	4

4.2. Структура дисциплины

№ п/п	Раздел дисциплины	Семестр	Формы текущего контроля успеваемости. Форма промежуточной аттестации			
			Лекции	Практические, групповые	СРС	
1	**2**	**3**	**4**	**5**	**6**	**7**
1.1	Понятие информационной безопасности.	*8*	2	4	2	Входной контроль (тест)
1.2	Угрозы безопасности.	*8*	2	4	2	
1.3	Основные принципы построения подсистемы защиты информации.	*8*	2	4	2	
2.1	Программно-технические меры обеспечения ИБ	*8*	2	4	2	
2.2	Защита информации от несанкционированного доступа.	*8*	4	4	2	Текущий контроль (компьютерное тестирование)
2.3	Криптография	*8*	2	4	2	
3.1	Разграничение доступа к информации в информационных системах.	*8*		12	2	
4.1	Правовое обеспечение информационной безопасности	*8*	4	2	2	
4.2	Административный уровень обеспечения информационной безопасности.	*8*	2		1	
4.3	Организационный уровень защиты информации	*8*	2	4	1	Текущий контроль (реферат)
5.1	Компьютерные вирусы.	*8*	2		2	
5.2	Антивирусное программное обеспечение.	*8*		6	2	
	Итого		24	48	26	
	Промежуточная аттестация –экзамен (4 часа)					

4.2.1. Теоретические занятия - занятия лекционного типа

№ п/п	Наименование тем	Содержание учебных вопросов	Кол-во часов
Раздел 1. Основы безопасности информационных систем.			
1	**Тема 1.1.** Понятие информационной безопасности.	Основные понятия и определения. Уровни обеспечения информационной безопасности.	2
2	**Тема 1.2.** Угрозы безопасности.	Угрозы информационной безопасности. Общие методы обеспечения информационной безопасности.	2
3	**Тема 1.3.** Основные принципы построения подсистемы защиты информации.	Принципы обеспечения информационной безопасности. Методы и средства обеспечения ИБ.	2
Раздел 2. Защита информации в ИС			
4	**Тема 2.1.** Программно-технические меры обеспечения ИБ	Программно-технические меры обеспечения ИБ. Подсистемы системы информационной безопасности.	2
5	**Тема 2.2.** Защита информации от несанкционированного доступа.	Идентификации и аутентификация в ИС. Парольная аутентификация. Управление доступом. Протоколирование и аудит.	4
6	**Тема 2.3.** Криптография	Шифрование. Проверка подлинности.	2
Раздел 3. Организация разноуровневого доступа в информационных системах			
7	**Тема 3.1.** Разграничение доступа к информации в информационных системах.	Лабораторное занятие №№ 1, 2, 3.	-
Раздел 4. Организационно-правовое обеспечение информационной безопасности			
8	**Тема 4.1.** Правовое обеспечение информационной безопасности	Правовые акты общего назначения. Специальные законы и нормативные акты в области ИБ. Закон "О Персональных данных".	4
9	**Тема 4.2.** Административный уровень обеспечения информационной безопасности.	Политика безопасности верхнего и нижнего уровня. Программа обеспечения ИБ.	2
10	**Тема 4.3.** Организационный уравень защиты информации	Методы и формы организационной защиты информации. Технические средства защиты информационных каналов.	2
Раздел 5. Антивирусная защита информации			
11	**Тема 5.1.** Компьютерные вирусы.	Классификация компьютерных вирусов. Методы антивирусной защиты.	2
12	**Тема 5.2.** Антивирусное программное обеспечение.	Лабораторное занятие №№ 1, 2.	-
ИТОГО			24

4.2.2. Занятия семинарского типа (практические и лабораторные работы)

№ п/п	Наименование тем	Содержание учебных вопросов	Кол-во часов

№ п/п	Наименование тем	Содержание учебных вопросов	Кол-во часов
Раздел 1. Основы безопасности информационных систем			
1	**Тема 1.1.** Понятие информационной безопасности.	Основные понятия и определения. Уровни обеспечения информационной безопасности.	4
2	**Тема 1.2.** Угрозы безопасности.	Угрозы информационной безопасности. Общие методы обеспечения информационной безопасности.	4
3	**Тема 1.3.** Основные принципы построения подсистемы защиты информации.	Принципы обеспечения информационной безопасности. Методы и средства обеспечения ИБ.	4
Раздел 2. Защита информации в информационных системах			
4	**Тема 2.1.** Программно-технические меры обеспечения ИБ	Программно-технические меры обеспечения ИБ. Подсистемы системы информационной безопасности.	4
5	**Тема 2.2.** Защита информации от несанкционированного доступа.	Идентификации и аутентификация в ИС. Парольная аутентификация. Управление доступом. Протоколирование и аудит.	4
6	**Тема 2.3.** Криптография	Шифрование. Проверка подлинности.	4
Раздел 3. Организация разноуровневого доступа в информационных системах			
7	**Тема 3.1.** Разграничение доступа к информации в информационных системах.	**Лабораторная 1. Организация разноуровневого доступа в ИС. Лабораторная 2. Организация разноуровневого доступа в ИС к общим ресурсам. Лабораторная 3. Реализация политики безопасности в ИС.**	12
Раздел 4. Организационно-правовое обеспечение информационной безопасности			
8	**Тема 4.1.** Правовое обеспечение информационной безопасности	Правовые акты общего назначения. Специальные законы и нормативные акты в области ИБ. Закон "О Персональных данных".	2
9	**Тема 4.2.** Административный уровень обеспечения информационной безопасности.	Политика безопасности верхнего и нижнего уровня. Программа обеспечения ИБ.	-
10	**Тема 4.3.** Организационный уравень защиты информации	Методы и формы организационной защиты информации. Технические средства защиты информационных каналов.	4
Раздел 5. Антивирусная защита информации			
11	**Тема 5.1.** Компьютерные вирусы.	Классификация компьютерных вирусов. Методы антивирусной защиты.	-
12	**Тема 5.2.** Антивирусное программное обеспечение.	**Лабораторная 4. Установка и настройка параметров антивирусного программного обеспечения. Лабораторная 5. Установка и настройка**	6

№ п/п	Наименование тем	Содержание учебных вопросов	Кол-во часов
		параметров сетевых экранов.	
ИТОГО			48

4.2.3. Самостоятельная работа

№ п/п	Наименование тем	Кол-во часов
Раздел 1. Основы безопасности информационных систем		
1	**Тема 1.1.** Понятие информационной безопасности.	2
2	**Тема 1.2.** Угрозы безопасности.	2
3	**Тема 1.3.** Основные принципы построения подсистемы защиты информации.	2
Раздел 2. Защита информации в информационных системах		
4	**Тема 2.1.** Программно-технические меры обеспечения ИБ	2
5	**Тема 2.2.** Защита информации от несанкционированного доступа.	2
6	**Тема 2.3.** Криптография	2
Раздел 3. Организация разноуровневого доступа в информационных системах		
7	**Тема 3.1.** Разграничение доступа к информации в информационных системах.	2
Раздел 4. Организационно-правовое обеспечение информационной безопасности		
8	**Тема 4.1.** Правовое обеспечение информационной безопасности	2
9	**Тема 4.2.** Административный уровень обеспечения информационной безопасности.	1
10	**Тема 4.3.** Организационный уровень защиты информации	1
Раздел 5. Антивирусная защита информации		
11	**Тема 5.1.** Компьютерные вирусы.	2
12	**Тема 5.2.** Антивирусное программное обеспечение.	2
13	Подготовка к экзамену	4
ИТОГО		26

5. Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, современных профессиональных баз данных и информационных справочных систем

5.1. Образовательные технологии

При реализации различных видов учебной работы по дисциплине «Управление доступом в информационных системах» используются следующие образовательные технологии:

1) Технологии проблемного обучения: проблемная лекция, практическое занятие в форме практикума.

2) Информационно-коммуникативные образовательные технологии: лекция-визуализация.

3) Инновационные методы, которые предполагают применение информационных образовательных технологий, а также учебно-методических материалов, соответствующих современному мировому уровню, в процессе преподавания дисциплины:

- использование медиаресурсов, энциклопедий, электронных библиотек и Интернет;
- консультирование студентов с использованием электронной почты4
- использование программно-педагогических тестовых заданий для проверки знаний обучающихся.

5.2. Лицензионное программное обеспечение

В образовательном процессе при изучении дисциплины используется следующее лицензионное программное обеспечение:

операционные системы	MS Windows 10 Professional SP1
	MS Windows 7 Professional SP1
	MS Windows Server 2016 Standard
офисные программы	MS Office 2013 Standart
	MS Project 2013
	Adobe Acrobat 11
базы данных	MS Access 2013
антивирусные пакеты	AVP Kaspersky Endpoint Security 11
система тестирования	INDIGO

5.3. Современные профессиональные базы данных

В образовательном процессе при изучении дисциплины используются следующие современные профессиональные базы данных:

Реферативная и справочная база данных рецензируемой литературы Scopus - https://www.scopus.com.

Политематическая реферативно-библиографическая и наукометрическая (библиометрическая) база данных Web of Science - https://apps.webofknowledge.com

Архив научных журналов НП Национальный Электронно-Информационный Консорциум (НЭИКОН) (arch.neicon.ru)

http://choose-it.ru/article/?id=1237 – информационно-образовательный портал для молодых специалистов ИТ

http://mirznanii.com/info/informatsionnye-sistemy-i-tekhnologii_113221 - Информационные системы и технологии

bdu.fstec.ru/vul – базы данных по угрозам компьютерной безопасности.

5.4. Информационные справочные системы

1.Справочная информационно-правовая система «КонсультантПлюс» (договор №СВ16-182).

6. Фонд оценочных средств

Типовые задания, база тестов и иные материалы, необходимые для оценки результатов освоения дисциплины (в том числе в процессе ее освоения), а также методические материалы, определяющие процедуры этой оценки приводятся в приложении 1 к рабочей программе дисциплины.

Универсальная система оценивания результатов обучения выполняется в соответствии с Положением о формах, периодичности и порядке проыедения текущего контроля успеваемости и промежуточной аттестации обучающихся в АНПОО «ККУ», утвержденным приказом директора от 03.02.2020 г. № 31 о/д и включает в себя системы оценок:

1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»,
2) «зачтено», «не зачтено»

При разработке оценочных средств преподавателем используются базы данных педагогических измерительных материалов, предоставленных ООО «Научно-исследовательский институт мониторинга качества образования».

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

7.1 Основная учебная литература

- Лазицкас, Е.А. Базы данных и системы управления базами данных : учебное пособие / Е.А. Лазицкас, И.Н. Загумённикова, П.Г. Гилевский. - Минск : РИПО, 2016. - 267 с. : ил. - Библиогр. в кн. - ISBN 978-985-503-558-0 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=463305
-Вичугова, А.А. Инструментальные средства информационных систем : учебное пособие / А.А. Вичугова. - Томск : Издательство Томского политехнического университета, 2015. - 136 с. : ил., табл., схем. - Библиогр. в кн.. - ISBN 978-5-4387-0574-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=442814

7.2 Дополнительная учебная литература

-Нестеров, С.А. Основы информационной безопасности : учебное пособие. - Санкт-Петербург. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040
-Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429070
Информационные технологии в юридической деятельности : учебное пособие / . - Москва : ЮНИТИ-ДАНА, 2014. - 335 с. : ил. - Библиогр. в кн. - ISBN 978-5-238-02548-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=447909
- Системный администратор (журнал).

7.3. Электронные образовательные ресурсы

Электронно-библиотечная система «Университетская Библиотека Онлайн» - https://biblioclub.ru/.
Научная электронная библиотека - www.elibrary.ru.
Научная библиотека открытого доступа - https://cyberleninka.ru

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»), необходимых для освоения дисциплины

1.https://www.ixbt.com/ — специализированный российский информационно-аналитический сайт с самыми актуальными новостями из сферы IT
2.https://3dnews.ru/ - Интернет издание - публикация новостей и аналитики в компьютерных технологиях, результатов тестирования компьютерной техники (видеокарт, мультимедиа, принтеров, сканеров и др.).
3.http://www.cnews.ru/ - издание о высоких технологиях. Информация о высоких технологиях.
4. https://compress.ru/ - Компьютер ПРЕСС – Обзор новостей компьютерной аналитики.
5. https://www.microsoft.com/ru-ru/learning/training.aspx /Учебные курсы по ИТ Microsoft
6. http://www.intuit.ru/ Интернет-университет информационных технологий («ИНТУИТ»)
7. http://www.elw.ru/ Журнал «e-Learning World – Мир электронного обучения»
8. https://www.it-world.ru Новости и аналитика рынка информационных технологий
9.https://www.osp.ru/ Все новости мира компьютеров и связи.
10. https://i-exam.ru/ - Единый портал интернет-тестирования в сфере образования

9. Требования к минимальному материально-техническому обеспечению, необходимому для осуществления образовательного процесса по дисциплине

Для изучения дисциплины используется мультимедийная аудитория. Мультимедийная аудитория оснащена современными средствами воспроизведения и визуализации любой

видео и аудио информации, получения и передачи электронных документов.

Для изучения дисциплины требуется мультимедийная техника. Специальных материально-технических средств: лабораторного оборудования, компьютерных классов и т.п., для преподавания дисциплины не требуется.

Во время лекционных занятий целесообразно использовать мультимедийную технику, так как практически ко всем лекциям разработаны слайдовые презентации, сопоставительные таблицы и другой материал, который можно продемонстрировать с помощью мультимедийного проектора. В связи с этим материально-техническое обеспечение дисциплины предполагает мультимедийное оборудование. Материально-техническая база должна соответствовать действующим санитарным и противопожарным нормам.

Минимальные требования к оргтехники:

Процессор: 1,2 ГГц и выше;

Оперативная память: 1 Г и выше;

Другие устройства: Звуковая карта, колонки и/или наушники;

Устройство для чтения DVD-дисков.

Реализация программы дисциплины требует наличия учебных кабинетов: кабинет технических средств информатизации, библиотека, читальный зал с выходом в сеть Интернет.

Для среднего профессионального образования.

Приложение 1
к рабочей программе дисциплины Управление доступом в информационных системах

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Управление доступом в информационных системах

1.1. Оценочные средства по итогам освоения дисциплины

1.1.1. Цель оценочных средств

Целью оценочных средств является установление соответствия уровня подготовленности обучающегося на данном этапе обучения требованиям рабочей программы по дисциплине «Управление доступом в информационных системах».

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Управление доступом в информационных системах». Перечень видов оценочных средств соответствует рабочей программе дисциплины.

Комплект оценочных средств включает контрольные материалы для проведения всех видов контроля в форме устного и письменного опроса, практических занятий, и промежуточной аттестации в форме вопросов и заданий к экзамену.

Структура и содержание заданий – задания разработаны в соответствии с рабочей программой дисциплины «Управление доступом в информационных системах».

1.1.2. Объекты оценивания – результаты освоения дисциплины

Объектом оценивания являются формируемые компетенции ОК1, 5, ПК1.1-1, 1.5.

Результатами освоения дисциплины являются:

- З-1основные задачи сопровождения информационной системы;
- З-2отказы системы;
- З-3восстановление информации в информационной системе;
- З-4принципы организации разноуровневого доступа в информационных системах, политику безопасности в современных информационных системах.

- У-1осуществлять сопровождение информационной системы, настройку под конкретного пользователя, согласно технической документации;
- У-2поддерживать документацию в актуальном состоянии;
- У-3идентифицировать технические проблемы, возникающие в процессе эксплуатации системы;
- У-4производить документирование на этапе сопровождения;
- У-5организовывать разноуровневый доступ пользователей информационной системы в рамках своей компетенции;
- У-6строить архитектурную схему организации;
- У-7осуществлять выбор модели построения информационной системы и программных средств;

- ПО-1инсталляции, настройки и сопровождения одной из информационных систем;

- ПО-2выполнения регламентов по обновлению, техническому сопровождению и восстановлению данных информационной системы;
- ПО-3сохранения и восстановления базы данных информационной системы;
- ПО-4организации доступа пользователей к информационной системе в рамках компетенции конкретного пользователя;
- ПО-5участия в экспериментальном тестировании информационной системы на этапе опытной эксплуатации и нахождения ошибок кодирования в разрабатываемых модулях информационной системы;
- ПО-6участия в оценке качества и экономической эффективности информационной системы;
- ПО-7модификации отдельных модулей информационной системы.

Таблица 1 - Перечень компетенций, формируемых в процессе освоения дисциплины с указанием этапов их формирования

№ п/п	Этапы формирования компетенций в процессе освоения дисциплины. (контролируемые модули, разделы, темы дисциплины (результаты по разделам))	Перечень компетенций. (код контролируемой компетенции (или её части) / и ее формулировка)	Планируемые результаты освоения дисциплины	Формы контроля, наименова-ние оценочного средства
1	Раздел 1. Основы безопасности информационных систем	ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес. ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ПК 1.1. Собирать данные для анализа использования и функционирования информационной системы, участвовать в составлении отчетной документации, принимать участие в разработке проектной документации на модификацию информационной системы. ПК 1.5. Разрабатывать фрагменты документации по	З-1основные задачи сопровождения информационной системы; З-2отказы системы; З3восстановление информации в информационной системе;	Входной контроль (тест)

		эксплуатации информационной системы и фрагменты методики обучения пользователей.		
2	Раздел 2. Защита информации в информационных системах	ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес. ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ПК 1.1. Собирать данные для анализа использования и функционирования информационной системы, участвовать в составлении отчетной документации, принимать участие в разработке проектной документации на модификацию информационной системы. ПК 1.5. Разрабатывать фрагменты документации по эксплуатации информационной системы и фрагменты методики обучения пользователей	У-1осуществлять сопровождение информационной системы, настройку под конкретного пользователя, согласно технической документации; У-2поддерживать документацию в актуальном состоянии; У-3идентифицировать технические проблемы, возникающие в процессе эксплуатации системы; У-4производить документирование на этапе сопровождения;	Текущий контроль (компьютерное тестирование)
3	Раздел 3. Организация разноуровневого доступа в информационных системах	ПК 1.1. Собирать данные для анализа использования и функционирования информационной системы, участвовать в составлении отчетной документации, принимать участие в разработке проектной документации на модификацию информационной	З-4 принципы организации разноуровневого доступа в информационных системах, политику безопасности в современных информационных системах. У-5организовывать разноуровневый доступ пользователей	

		системы. ПК 1.5. Разрабатывать фрагменты документации по эксплуатации информационной системы и фрагменты методики обучения пользователей	информационной системы в рамках своей компетенции; У-6строить архитектурную схему организации; У-7осуществлять выбор модели построения информационной системы и программных средств	
4	Раздел 4. Организационно-правовое обеспечение информационной безопасности	ПК 1.1. Собирать данные для анализа использования и функционирования информационной системы, участвовать в составлении отчетной документации, принимать участие в разработке проектной документации на модификацию информационной системы. ПК 1.5. Разрабатывать фрагменты документации по эксплуатации информационной системы и фрагменты методики обучения пользователей	ПО-3сохранения и восстановления базы данных информационной системы; ПО-4организации доступа пользователей к информационной системе в рамках компетенции конкретного пользователя;	Текущий контроль (реферат)
5	Раздел 5. Антивирусная защита информации	ПК 1.1. Собирать данные для анализа использования и функционирования информационной системы, участвовать в составлении отчетной документации, принимать участие в разработке проектной документации на модификацию информационной системы. ПК 1.5. Разрабатывать фрагменты документации по эксплуатации	ПО-1инсталляции, настройки и сопровождения одной из информационных систем; ПО-2выполнения регламентов по обновлению, техническому сопровождению и восстановлению данных информационной системы; ПО-5участия в экспериментальном тестировании информационной системы на этапе	Промежуточная аттестация (экзамен)

		информационной системы и фрагменты методики обучения пользователей	опытной эксплуатации и нахождения ошибок кодирования в разрабатываемых модулях информационной системы; ПО-6участия в оценке качества и экономической эффективности информационной системы; ПО-7модификации отдельных модулей информационной системы.	

1.1.3. Формы контроля и оценки результатов освоения

Контроль и оценка результатов освоения – это выявление, измерение и оценивание знаний и умений формирующихся компетенций в рамках освоения дисциплины. В соответствии с учебным планом и рабочей программой дисциплины «Управление доступам в информационных системах» предусматривается входной, текущий, рубежный и итоговый контроль результатов освоения (промежуточная аттестация в форме экзамена).

1.2. Примерные (типовые) контрольные задания или иные материалы, необходимые для оценки знаний, умений, владений (или опыта деятельности), в процессе освоения дисциплины (модуля, практики), характеризующих этапы формирования компетенций в процессе освоения дисциплины

1.2.1. Примерные (типовые) контрольные задания или иные материалы для проведения входного контроля

Тест (на уровне знаний)

Информационные технологии (ОК 1, 5, ПК 1.1.)

1. **По способу восприятия информации человеком различают следующие виды информации:**
   a) текстовую, числовую, символьную, графическую, табличную и пр.,
   b) научную, социальную, политическую, экономическую, религиозную и пр.,
   c) обыденную, производственную, техническую, управленческую,
   d) визуальную, звуковую, тактильную, обонятельную, вкусовую,
   e) математическую, биологическую, медицинскую, психологическую и пр.

2. **По области применения информацию можно условно разделить на:**
   a) текстовую и числовую,
   b) визуальную и звуковую,
   c) графическую и табличную,
   d) научную и техническую,
   e) тактильную и вкусовую.

3. **К свойству информации НЕ относится:**
   a) доступность,

b) полезность,
c) активность
d) достоверность,
e) полнота.

4. Концепция информационного хранилища может быть реализована в нескольких вариантах:
a) централизованное хранилище данных;
b) распределенное хранилище данных;
c) корпоративное хранилище данных;
d) единое интегрированное хранилище.

5. Автоматизированное рабочее место (АРМ) – это:
a) программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида;
b) технический комплекс, предназначенный для автоматизации деятельности определенного вида;
c) программный комплекс, предназначенный для автоматизации деятельности определенного вида;
d) аппаратная платформа, предназначенный для автоматизации деятельности определенного вида.

6. Информационная инфраструктура охватывает
a) вычислительную технику;
b) средства коммуникации;
c) методическое и программное обеспечение, технологии;
d) вспомогательные виды деятельности;
e) все вышеперечисленное.

7. Наиболее простой функцией АРМ является …
a) информационно-справочное обслуживание;
b) моделирование ситуаций;
c) аналитическое прогнозирование;
d) принятие решений;
e) нет правильного ответа.

8. Эффективным режимом работы АРМ является его функционирование в рамках локальной вычислительной сети в качестве …
a) рабочей станции;
b) сервера;
c) персонального компьютера;
d) локальной машины;
e) нет правильного ответа.

Устройство и функционирование информационной системы

a) Автоматизированная информационная система (АИС) - это:
b) Совокупность информации, экономико-математических методов и моделей, технических, программных, технологических средств и специалистов, предназначенную для обработки информации и принятия управленческих решений;

c) Совокупность технических, программных и информационных ресурсов, обеспечивающая конечному пользователю обработку данных и автоматизацию управленческих функций в конкретной предметной области;.
d) Системно-организованная для решения задач управления совокупность методов и средств реализации операций сбора, регистрации, передачи, накопления, обработки и защиты информации на базе применения по, используемых средств вт и связи;
e) Все определения верны.

9. Автоматизированная информационная технология - это:
f) Совокупность информации, экономико-математических методов и моделей, технических, программных, технологических средств и специалистов, предназначенную для обработки информации и принятия управленческих решений;
g) Совокупность технических, программных и информационных ресурсов, обеспечивающая конечному пользователю обработку данных и автоматизацию управленческих функций в конкретной предметной области;
h) Системно-организованная для решения задач управления совокупность методов и средств реализации операций сбора, регистрации, передачи, накопления, обработки и защиты информации на базе применения по, используемых средств ВТ и связи;
i) Все определения верны.

10. В модели сервера базы данных (DBS) прикладные программы выполняются на…
a) Сервере;
b) Клиенте
c) Маршрутизаторе;
d) Концентраторе.

11. В модели доступа к удаленным данным (RDA) прикладные программы выполняются на:
a) Сервере;
b) Клиенте
c) Маршрутизаторе;
d) Концентраторе.

12. Каковы требования к организации внутримашинной информационной базы
a) База должна быть минимально избыточна;
b) В базе допускается избыточность информации в распределенных системах
c) В базе не допускается избыточность информации в распределенных системах;
d) База должна быть максимально избыточна.

Операционные системы

13. Кэш-памятью называют…
a) метод несовместного использования запоминающих устройств;
b) метод совместного использования одного типа запоминающих устройств;
c) **метод совместного использования двух типов запоминающих устройств;**
d) верного ответа нет

14. Виртуальная память решает следующие задачи:
a) предоставляет системе оперативную память, размер которой меньше физической оперативной памяти;
b) запрещает предоставлять системе оперативную память, размер которой превышает

физическую оперативную память;

c) предоставляет системе оперативную память, размер которой превышает физическую оперативную память.

d) всё перечисленное

15. На 32-разрядных процессорах максимально возможно адресовать памяти:

a) до 4 либо до 32 Гб;

b) до 4 либо до 64 Гб;

c) до 4 либо до 128Гб;

d) до 4 либо до 256Гб

16. К какому классу можно отнести операционную систему MS DOS?

a) однозадачная, однопользовательская;

b) многозадачная, многопользовательская;

c) реального режима времени;

d) система особого класса

17. Наиболее быстрым запоминающим устройство является…

a) ОЗУ;

b) ПЗУ;

c) регистры процессора;

d) верного ответа нет

Компьютерные сети

18. Сеть имеет следующие параметры:

a. ПК подключаются к общему концентратору;

b. передача данных осуществляется любым узлом, в любое время одновременно для всех остальных узлов через концентратор;

c. среда передачи – витая пара;

Определить топологию.

- Шина
- **Звезда**
- Кольцо
- Снежинка

19. Метод доступа CSMA/CD это…

- множественный доступ с прослушиванием несущей и избеганием коллизий
- **множественный доступ с прослушиванием несущей и обнаружением коллизий**
- детерминированный доступ

20. Расставить соответствие между сетевое технологией и применяемым методом доступа.

- Методы доступа:
    a. CSMA/CA
    b. CSMA/CD
    c. По маркеру
- Сетевые технологии:
    a. Local Talk
    b. Ethernet
    c. Token Ring

21. Устройство предназначенное для объединения подсетей, разделяя при этом их внутренний трафик и ограничивая широковещательные посылки называется.

a) Маршрутизатор
b) Принт-сервер
c) Медиаконвертер
d) Межсетевой экран
e) Коммутатор
f) Концентратор

22. Устройство предназначенное для увеличения размера сети (кол-ва ПК) и обеспечивающее прием, усиление кадра данных на одном порту и передачу его на все остальные называется.

a) Концентратор
b) Маршрутизатор
c) Принт-сервер
d) Медиаконвертер
e) Межсетевой экран
f) Коммутатор

23. Устройство предназначенное для увеличения размера сети (кол-ва ПК) и обеспечивающее прием, усиление кадра данных на одном порту и передачу его только на порт назначения называется.

a) Коммутатор
b) Маршрутизатор
c) Принт-сервер
d) Медиаконвертер
e) Межсетевой экран
f) Концентратор

24. Сеть имеет следующие параметры:

a. ПК подключаются последовательно друг к другу;
b. передача данных осуществляется любым узлом, в любое время одновременно для всех остальных узлов;
c. среда передачи – коаксиальный кабель;

Определить топологию.

- **Шина**
- Звезда
- Кольцо
- Снежинка

25. Сеть имеет следующие параметры:

a. ПК подключаются к общему концентратору;
b. передача данных осуществляется для каждого узла строго по очереди по специальному маркеру формируемому концентратором;
c. среда передачи – коаксиальный кабель или витая пара;

Определить топологию.

- Шина
- Звезда
- **Кольцо**
- Снежинка

Критерии оценивания тестов

% правильных ответов	Оценка по традиционной системе
85-100	Отлично
70-84	Хорошо

50-69	Удовлетворительно
0-49	Неудовлетворительно

1.2.2. Примерные (типовые) контрольные задания или иные материалы для проведения текущего контроля

Компьютерное тестирование (ОК 1, 5, ПК 1.1, 1.5)

Раздел 1. Основы безопасности информационных систем. Раздел 2. Защита информации в ИС.
Раздел 3. Организация разноуровневого доступа в информационных системах.
Раздел 4. Организационно-правовое обеспечение информационной безопасности.
Раздел 5. Антивирусная защита информации.

1.2.3. Примерные (типовые) контрольные задания или иные материалы для проведения текущего контроля

Примерная тематика рефератов (ОК 1, 5, ПК 1.1, 1.5)
(на уровне умений)

1. Современное антивирусное ПО.
2. Аппаратные средства защиты сети.
3. Аппаратные средства защиты ПК от несанкционированного доступа.
4. Программные средства шифрования данных.

Требования к оформлению реферата

1. Титульный лист с названием учебного заведения, темы реферата, фамилии и инициалов автора работы, а также фамилии, инициалов, ученой степени руководителя, населенного пункта, года написания работы.
2. Оглавление (план реферата) с указанием вопросов и номеров страниц. Страницы должны проставляться на всех листах реферата кроме титульного листа. Каждая глава (раздел) должны начинаться с новой страницы. В реферате должно быть не менее двух глав.
3. Библиография (использованные источники) должна оформляться в соответствии с Гостом.
4. Объем работы – 10-15 страниц (без приложений).

Критерии оценивания реферата

Оценка	***Критерии оценки***
«отлично»	Если выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему, логично изложена собственная позиция, сформулирован выводы. Студент свободно ориентируется в тексте, на защите реферата рассказывает, а не читает доклад, отвечает на вопросы преподавателя.
«хорошо»	Основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала: отсутствует логическая последовательность в суждениях, не выдержан объем реферата,

	имеются упущения в оформлении, на дополнительные вопросы при защите даны неполные ответы.
«удовлетворительно»	Имеются существенные отступления от требований к оформлению реферата. Тема освещена лишь частично, допущены фактические ошибка в содержании реферата или при ответе на дополнительные вопросы. Отсутствуют выводы.
«неудовлетворительно»	Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

1.2.4. Примерные (типовые) контрольные задания или иные материалы для проведения промежуточной аттестации

Примерные (типовые) вопросы к экзамену по дисциплине «Управление доступом в информационных системах»

Вопрос	Код компетенции *(согласно РПД)*
1. Свойства информации.	ОК 1, 5, ПК 1.1, 1.5
2. Угрозы информационной безопасности.	ОК 1, 5, ПК 1.1, 1.5
3. Принципы обеспечения информационной безопасности.	ОК 1, 5, ПК 1.1, 1.5
4. Программно-технические меры ИБ.	ОК 1, 5, ПК 1.1, 1.5
5. Методы обеспечения ИБ.	ОК 1, 5, ПК 1.1, 1.5
6. Средства защиты информационных систем.	ОК 1, 5, ПК 1.1, 1.5
7. Классификация сетевых атак на ИС.	ОК 1, 5, ПК 1.1, 1.5
8. Меры по обеспечению надежности парольной защиты.	ОК 1, 5, ПК 1.1, 1.5
9. Симметричное шифрование.	ОК 1, 5, ПК 1.1, 1.5
10. Ассиметричное шифрование.	ОК 1, 5, ПК 1.1, 1.5
11. Контроль целостности (ЭЦП).	ОК 1, 5, ПК 1.1, 1.5
12. Цифровые сертификаты.	ОК 1, 5, ПК 1.1, 1.5
13. Правовые акты общего назначения в области ИБ.	ОК 1, 5, ПК 1.1, 1.5
14. Специальные законы и нормативные акты в области ИБ.	ОК 1, 5, ПК 1.1, 1.5

№ билета	Содержание билета	Код компетенции *(согласно РПД)*
Билет 1	1. Основные понятия информационной безопасности. 2. Подсистема «Управления доступом». 3. Настроить сеть доменного типа с выделенным контроллером домена и сервером DNS.	ОК 1, 5, ПК 1.1, 1.5
Билет 2	1. Проблемы информационной безопасности. (ОК 1, 5, ПК 1.1,	ОК 1, 5, ПК 1.1, 1.5

	1.5) 2. Подсистема «Протоколирования и аудита». 3. Подключить к домену виртуальную рабочую станцию на базе ОС Windows XP.	
Билет 3	1. Свойства информации. 2. Основные понятия криптографии. 3. Создать учётную запись пользователя, группу и организационное подразделение.	ОК 1, 5, ПК 1.1, 1.5
Билет 4	1. Понятие доступности информации. 2. Способы шифрования. 3. Создать общие ресурсы на сервере и настроить права доступа.	ОК 1, 5, ПК 1.1, 1.5
Билет 5	1. Понятие целостности информации. 2. Симметричное шифрование. 3. Создать перемещаемый профиль пользователя «Фамилия-1» (Профиль хранится на сервере в папке /**Экзамен №группы**/).	ОК 1, 5, ПК 1.1, 1.5
Билет 6	1. Понятие конфиденциальности информации. 2. Ассиметричное шифрование. 3. Создать обязательный перемещаемый профиль пользователя «Фамилия» (Профиль хранится на сервере в папке /**Экзамен №группы/**).	ОК 1, 5, ПК 1.1, 1.5
Билет 7	1. Подходы к обеспечению информационной безопасности. 2. Понятие «Проверка подлинности» . 3. Назначить созданным пользователям сетевые домашние папки (разместить их в сетевой папке /**Домашняя «своя фамилия»/** на сервере) .	ОК 1, 5, ПК 1.1, 1.5
Билет 8	1. Понятие угрозы информационной безопасности. 2. Понятие «Цифровые сертификаты» . **3.** Назначить пользователю «Фамилия-1» общую скрытую сетевую папку **/ОБЩАЯ_Скрытая/** (в качестве сетевого именем использовать свои инициалы «ФИО» набранные латиницей) расположенную на сервере и подключающуюся в качестве сетевого диска **Z**.	ОК 1, 5, ПК 1.1, 1.5
Билет 9	1. Классификация угроз ИБ. 2. Меры законодательного уровня ИБ 3. Настроить групповые политики в соответствии со следующими правилами.	ОК 1, 5, ПК 1.1, 1.5
Билет 10	1. Вредоносное программное обеспечение. Правовые акты общего назначения в области ИБ. 2. Для созданных пользователей создать групповую политику «Ограничения Фамилия» и настроить следующим образом.	ОК 1, 5, ПК 1.1, 1.5
Билет 11	1. Понятие атаки на информационную систему. 2. Специальные законы и нормативные акты в области ИБ. 3. Используя программу Private Disk создать виртуальный зашифрованный диск со следующими параметрами.	ОК 1, 5, ПК 1.1, 1.5
Билет 12	1. Классификация атак. 2. Административный уровень защиты информации. 3. Выполнить шифрование и дешифрование с помощью программы **Norton Sec.**	ОК 1, 5, ПК 1.1, 1.5
Билет 13	1. Пассивная атака. 2. Политика безопасности верхнего уровня. 3. Выполнить шифрование и дешифрование с помощью программы **MNT**.	ОК 1, 5, ПК 1.1, 1.5
Билет 14	1. Активная атака. 2. Политика безопасности среднего уровня. 3. Выполнить шифрование и дешифрование с помощью программы **Blowfish**.	ОК 1, 5, ПК 1.1, 1.5
Билет 15	1. Принципы обеспечения информационной безопасности. 2. Политика безопасности нижнего уровня. 3. Выполнить шифрование и дешифрование с помощью программы **Gifitup**.	ОК 1, 5, ПК 1.1, 1.5
Билет 16	1. Понятие «Системность ИБ». 2. Подсистема «Управления доступом». 3. Выполнить шифрование и дешифрование с помощью программы **S-Tools**.	ОК 1, 5, ПК 1.1, 1.5
Билет 17	1. Понятие «Комплексность ИБ». 2. Подсистема «Протоколирования и аудита». 3. Настроить сеть доменного типа с выделенным контроллером домена и сервером DNS.	ОК 1, 5, ПК 1.1, 1.5

Билет 18	1. Понятие «Непрерывность защиты ИБ» . 2. Основные понятия криптографии. 3. Подключить к домену виртуальную рабочую станцию на базе ОС Windows XP.	ОК 1, 5, ПК 1.1
Билет 18	1. Понятие «Разумная достаточность ИБ» . 2. Способы шифрования. 3. Создать учётную запись пользователя, группу и организационное подразделение.	ОК 1, 5, ПК 1.1, 1.5
Билет 20	1. Понятие «Гибкость управления и применения ИБ» . 2. Симметричное шифрование. 3. Создать общие ресурсы на сервере и настроить права доступа.	ОК 1, 5, ПК 1.1 ОК 1, 5, ПК 1.1, 1.5, 1.5
Билет 21	1. Понятие «Открытость алгоритмов и механизмом защиты ИБ». 2. Ассиметричное шифрование. Создать перемещаемый профиль пользователя «Фамилия-1» (Профиль хранится на сервере в папке **/Экзамен №группы/**).	ОК 1, 5, ПК 1.1, 1.5
Билет 22	1. Понятие «Простота применения защитных мер и средств ИБ» . 2. Понятие «Проверка подлинности». 3. Создать обязательный перемещаемый профиль пользователя «Фамилия-2» (Профиль хранится на сервере в папке **/Экзамен №группы/**).	ОК 1, 5, ПК 1.1, 1.5
Билет 23	1. Методы обеспечения ИБ. 2. Понятие «Цифровые сертификаты»,. 3. Назначить созданным пользователям сетевые домашние папки (разместить их в сетевой папке **/Домашняя «своя фамилия»/** на сервере).	ОК 1, 5, ПК 1.1, 1.5
Билет 24	1. Средства защиты информационных систем. **2.** Меры законодательного уровня ИБ. Назначить пользователю «Фамилия-1» общую скрытую сетевую папку **/ОБЩАЯ_Скрытая/** (в качестве сетевого именем использовать свои инициалы «ФИО» набранные латиницей) расположенную на сервере и подключающуюся в качестве сетевого диска **Z.**	ОК 1, 5, ПК 1.1, 1.5
Билет 25	1. Программно-технические меры обеспечения ИБ. 2. Правовые акты общего назначения в области ИБ. (3. Настроить групповые политики в соответствии со следующими правилами.	ОК 1, 5, ПК 1.1, 1.5

Примеры тестовых заданий

(на уровне умений)

Содержание заданий	Код компетенции *(согласно РПД)*
1. Основные свойства информации. **1. <u>Доступность</u>** **2. <u>Целостность</u>** **3. <u>Конфиденциальность</u>** 4. Скрытость 5. Непрерывность	ОК 1, 5, ПК 1.1, 1.5
2. Возможность получения информации или информационной услуги за приемлемое время это… **1. <u>Доступность</u>** 2. Целостность 3. Конфиденциальность	ОК 1, 5, ПК 1.1, 1.5
3. Актуальность и непротиворечивости информации, ее защищенность от разрушения и несанкционированного изменения это...	ОК 1, 5, ПК 1.1, 1.5

1. Доступность **2. <u>Целостность</u>** 3. Конфиденциальность	
4. Информация раскрытие содержимого которой может привести к ущербу (экономическому, моральному) организации или физического лица называется... **1. <u>Предметной</u>** 2. Служебной 3. Системной	ОК 1, 5, ПК 1.1, 1.5
5. Информация (например: пароли пользователей) не относящаяся к определенной предметной области, однако раскрытие которой может привести к несанкционированному доступу ко всей информации называется… 1. Предметной **2. <u>Служебной</u>** 3. Системной 6. Код обладающий способностью к распространению путем внедрения в другие программы... **1. <u>Вирус</u>** 2. Червь 3. Троян	ОК 1, 5, ПК 1.1, 1.5
7. Код способный самостоятельно вызывать распространение своих копий по ИС и их выполнение... 1. Вирус **2. <u>Червь</u>** 3. Троян	ОК 1, 5, ПК 1.1, 1.5
8. Программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к "зависанию", воруют конфиденциальную информацию называются... 1. Вирус 2. Червь **3. <u>Троян</u>**	ОК 1, 5, ПК 1.1, 1.5
9. Атаки по воздействию на информационную систему классифицируются... 1. Локальные атаки 2. Удаленные атаки **3. <u>Активные атаки</u>** **4. <u>Пассивные атаки</u>**	ОК 1, 5, ПК 1.1, 1.5
10. Атаки по месту возникновения в информационной системе классифицируются как... **1. <u>Локальные атаки</u>** **2. <u>Удаленные атаки</u>** 3. Активные атаки 4. Пассивные атаки	ОК 1, 5, ПК 1.1, 1.5
11. Атака, при которой противник не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между	ОК 1, 5, ПК 1.1, 1.5

отправителем и получателем свои сообщения называется... 1. Локальной 2. Удаленной 3. Активной **4. Пассивной**	
12. Атака целью которой может быть только прослушивание передаваемых сообщений и анализ трафика называется... 1. Локальной 2. Удаленной 3. Активной **4. Пассивной**	ОК 1, 5, ПК 1.1, 1.5
13. Атака, при которой противник имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения называется... (ОК 1, 1. Локальной 2. Удаленной 3. Активной 4. Пассивной	ОК 1, 5, ПК 1.1, 1.5
14. Выберите метод физического преграждения пути злоумышленнику к информации... **1. Препятствие** 2. Маскировка 3. Управление доступом 4. Регламентация 5. Принуждение	ОК 1, 5, ПК 1.1, 1.5
15. Выберите метод защиты с помощью регулирования использования информационных ресурсов системы... 1. Препятствие 2. Маскировка **3. Управление доступом** 4. Регламентация 5. Принуждение	ОК 1, 5, ПК 1.1, 1.5
16. Выберите метод защиты информации путем ее криптографического преобразования: 1. Препятствие **2. Маскировка** 3. Управление доступом 4. Регламентация 5. Принуждение	ОК 1, 5, ПК 1.1, 1.5
17. Выберите метод защиты информации, создающий условия автоматизированной обработки, при которых возможности несанкционированного доступа сводится к минимуму: 1. Препятствие 2. Маскировка 3. Управление доступом **4. Регламентация** 5. Принуждение	ОК 1, 5, ПК 1.1, 1.5
18. Выберите метод защиты, при котором персонал вынужден соблюдать правила обработки, передачи и использования информации: 1. Препятствие 2. Маскировка	ОК 1, 5, ПК 1.1, 1.5

3. Управление доступом 4. Регламентация **5. <u>Принуждение</u>**	
19. Различные электрические, электронные и компьютерные устройства относятся к _____ средствам защиты информационных систем. **1. <u>Техническим</u>** 2. Физическим 3. Программным 4. Криптографическим 5. Организационным 6. Законодательным	ОК 1, 5, ПК 1.1, 1.5
20. В виде автономных устройств и систем реализуются _____ средства защиты информационных систем. 1. Технические **2. <u>Физические</u>** 3. Программные 4. Криптографические	ОК 1, 5, ПК 1.1, 1.5
21. Математические алгоритмы, обеспечивающие преобразования данных для решения задач информационной безопасности называются _____ средствами защиты информационных систем. 1. Физическим 2. Программным **3. <u>Криптографическим</u>** 4. Организационным	ОК 1, 5, ПК 1.1, 1.5
22.Совокупность организационно-технических и организационно-правовых мероприятий направленных на решение задач информационной безопасности называются _____ средствами защиты информационных систем. 1. Техническим 2. Физическим 3. Программным **4. <u>Организационным</u>** 5. Законодательным	ОК 1, 5, ПК 1.1, 1.5
23.Классификация мер безопасности на основе сервисов безопасности и их места в общей архитектуре ИС: (Установить последовательность правильных ответов). (ОК 1, 5, ПК 1.1, 1.5) **1. Превентивные** **2. Меры обнаружения нарушений** **3. Локализующие зону воздействия** **4. Меры по выявлению нарушений** **5. Меры восстановления режима безопасности**	ОК 1, 5, ПК 1.1, 1.5
24. Комплексный подход, применяемый при построении СОБИ, предусматривает наличие нескольких уровней защиты, которые определяют требования по обеспечению безопасности информации на всех этапах ее обращения в КИС: **1. <u>Технологического,</u>** **2. <u>Пользовательского,</u>** **3. <u>Сетевого</u>** **4. <u>Канального</u>** 5. Информационного 6. Предварительного	ОК 1, 5, ПК 1.1, 1.5

25. Подсистема _____ предназначена для поддержания целостной программно-аппаратной среды КИС, обеспечения гарантий доверительности пользователей КИС к предоставляемой системой информации и сервисам. **1. <u>Поддержки доверенной информационной среды</u>** 2. Аутентификации и идентификации 3. Контроля доступа 4. Аудита и регистрации	ОК 1, 5, ПК 1.1, 1.5

Приложение 2
к рабочей программе
дисциплины Управление
доступом в
информационных системах

Методические рекомендации и указания

1. Методические указания для обучающихся по освоению дисциплины

Дисциплина «Управление доступом в информационных системах» считается освоенной обучающимся, если он имеет положительные результаты входного, текущего контроля и промежуточной аттестации.

Для достижения вышеуказанного обучающийся должен соблюдать следующие правила, позволяющие освоить дисциплину на высоком уровне:

1. Начало освоения курса должно быть связано с изучением всех компонентов программы дисциплины «Управление доступом в информационных системах» с целью понимания ее содержания и указаний, которые будут доведены до сведения обучающегося на первой лекции и первом занятии семинарского типа.

Перед началом курса целесообразно ознакомиться со структурой дисциплины на основании программы, а так же с последовательностью изучения тем и их объемом. С целью оптимальной самоорганизации необходимо сопоставить эту информацию с графиком занятий и выявить наиболее затратные по времени и объему темы, чтобы заранее определить для себя периоды объемных заданий.

2. Каждая тема содержит лекционный материал, список литературы для самостоятельного изучения, вопросы и задания для подготовки к занятиям семинарского типа. Необходимо заранее обеспечить себя этими материалами и литературой или доступом к ним.

3. После лекции необходимо изучить лекционный материал по соответствующей теме, обратить особое внимание на актуальные и проблемные вопросы рассматриваемой темы.

4. Занятие семинарского типа, как правило, начинается с опроса по лекционному материалу темы и материалам указанных к теме литературных источников. В связи с этим подготовка к практическому занятию заключается в повторении лекционного материала и изучении вопросов предстоящего занятия.

При возникновении затруднений с пониманием материала занятия обучающийся должен обратиться с вопросом к преподавателю для получения соответствующих разъяснений в отведенное для этого преподавателем время на занятии либо по электронной почте. В интересах обучающегося своевременно довести до сведения преподавателя информацию о своих затруднениях в освоении предмета и получить необходимые разъяснения.

5. Подготовка к экзамену является заключительным этапом изучения дисциплины. Экзамен проводится в устной форме. Каждый билет содержит по три вопроса: два – теоретических, один – практическое задание (или тесты).

Содержание вопросов находится в доступном режиме с начала изучения дисциплины. В связи с этим целесообразно изучать вопросы не в период экзаменационной сессии непосредственно в дни перед экзаменом, а по каждой теме вместе с подготовкой к соответствующему текущему занятию. Кроме того необходимо помнить, что часть вопросов (не более 10%) непосредственно перед экзаменом может быть дополнена или изменена. В связи с этим целесообразно изучать не только вопросы, выносимые на экзамен, но и иные вопросы, рассматриваемые на лекциях и занятиях семинарского типа.

2. Методические указания к выполнению лабораторных работ

Методические указания включают в себя материал 2 лабораторных работ дисциплины.

Для успешного освоения дисциплины должны быть сформированы компетенции ОК 5, ОК 6, ПК-1.8, ПК-1.7 на пороговом уровне, и преследуют цель обучить студентов навыкам работы с операционной системой Windows и сетевым возможностям операционной системы Windows.

Общие для всех лабораторных работ пункты приведены ниже.

Аппаратура и материалы.

Лабораторный практикум выполняется в штатном компьютерном классе, оборудованном IBM – совместимыми персональными компьютерами под управлением операционной системы Windows XP/7.

Указания по технике безопасности.

Включение и выключение ПЭВМ и дисплеев производить только по команде преподавателя.

В случае появления опасного для жизни напряжения на корпусе машины немедленно доложить преподавателю и, никого не допуская к данному дисплею, выключить пакетный выключатель, находящийся у выхода из аудитории.

3.Методические указания по подготовке к сдаче экзамена

Экзамен является итоговой формой контроля знаний обучающегося по «Управление доступом в информационных системах», способом оценки результатов его учебной деятельности. Основной целью экзамена является проверка степени усвоения полученных обучающимся знаний и их системы.

Для успешной сдачи экзамена необходимо продемонстрировать разумное сочетание знания и понимания учебного материала. На экзамене проверяется не столько механическое запоминание обучающимся изложенной информации, сколько его способность её анализировать, объяснять, аргументировать и отстаивать свою позицию.

К экзамену целесообразно готовиться с самого начала учебного цикла, поскольку только систематическая подготовка может обеспечить формирование у обучающегося качественных системных знаний.

При подготовке следует пользоваться комплексом различных источников - не только конспектами лекций, материалами по подготовке к семинарским занятиям, но также и учебной, научной, справочной литературой.

Преподаватель вправе задать на экзамене обучающемуся наводящие, уточняющие и дополнительные вопросы в рамках билета.

Основными критериями, которыми преподаватель руководствуется при оценке знаний, являются следующие:

- соответствие ответа обучающегося теме вопросов;
- умение строить ответ полно, но лаконично с акцентом на наиболее важных моментах;

- степень осведомлённости о научных и нормативных источниках;
- умение связывать теорию с практикой;
- приведение конкретных примеров.

Рекомендации по проведению учебных занятий с обучающимися с применением электронного обучения и дистанционных образовательных технологий

Для проведения контактной работы обучающихся с преподавателем АНПОО «ККУ» с применением электронного обучения и дистанционных образовательных технологий определен набор электронных ресурсов и приложений, которые рекомендуются к использованию в образовательном процессе. Образовательный процесс осуществляется в соответствии с расписанием учебных занятий 2023/2024 учебного года, размещенным на официальном сайте колледжа.

Организация образовательного процесса осуществляется через личный кабинет на официальном сайте колледжа. Преподаватель в электронном журнале для соответствующей учебной группы указывает тему занятия. Прикрепляет учебные материалы, задания или ссылки на электронные ресурсы, необходимые для освоения темы, выполнения домашних заданий.

Алгоритм дистанционного взаимодействия:

1.1. Для обеспечения дистанционной связи с обучающимися преподаватель взаимодействуют с обучающимися групп в электронной платформе Сферум, либо посредством корпоративной электронной почты (домен @kiu39.ru/ @kku39.ru).

1.2. В сформированных группах обучающихся на платформах (см. выше) преподаватель доводит до обучающихся информацию:

-об алгоритме размещения информации об учебных материалах и заданиях на электронных ресурсах колледжа.

- индивидуальный график консультирования обучающихся, в т.ч. дистанционном формате.

1.3. Обучающиеся выполняют задание, в соответствии с расписанием учебных занятий в формате ДО и предоставляют их в электронной форме на электронный ресурс.

1.4. Осуществление мониторинга выполнения учебного плана и посещаемости занятий происходит ежедневно преподавателем через электронные ресурсы.