МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5BFEE1D286E9C95A0C0D2C611E434BD5
Владелец: Степанченко Алексей Леонидович
Действителен: с 23.09.2026 по 17.12.2027

«УТВЕРЖДАЮ»
Проректор
А. Л. Степанченко
24 марта 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «Б1.В.06 АРХИТЕКТУРА ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

Уровень высшего образования: магистратура

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль) подготовки: Защита информации в геоинформационных системах и системах сбора пространственных данных

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Год набора (приема на обучение): 2025

Срок получения образования: 2 года

Объем: в зачетных единицах: 5 з.е.
в академических часах: 180 ак.ч.

Москва, 2025

Разработчики:
Доцент кафедры Информационно-измерительных систем, к.т.н.
Тележников В. Ю.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки от 26.11.2020 № 1455

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.10.2024, № 10-24

Содержание

1. Цель и задачи освоения дисциплины (модуля)

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

3. Место дисциплины в структуре ОП

4. Объем дисциплины и виды учебной работы

5. Содержание дисциплины
   5.1. Разделы, темы дисциплины и виды занятий
   5.2. Содержание разделов, тем дисциплины и формы текущего контроля

6. Оценочные материалы текущего контроля

7. Оценочные материалы промежуточной аттестации

8. Порядок проведения промежуточной аттестации

9. Материально-техническое и учебно-методическое обеспечение дисциплины
   9.1. Перечень основной и дополнительной учебной литературы
   9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся
   9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине
   9.4. Оборудование и технические средства обучения

10. Методические указания по освоению дисциплины (модуля)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - сформировать способность разрабатывать согласованные проектные решения по защите автоматизированных систем: определять защищаемые данные и правила доступа, выбирать архитектуру сети и механизмы защиты, обосновывать отказоустойчивость и оформлять проверяемые требования и проектные документы.

Задачи изучения дисциплины:

- освоить классификацию защищаемых сведений, различие правовых режимов ограничения доступа и выделение субъектов и объектов защиты;
- научиться связывать требования безопасности с организационными правилами, техническими механизмами и проверками их выполнения;
- освоить организацию разработки защищенной АС, согласование коллективных изменений и приемочных испытаний;
- получить опыт выбора и реализации архитектуры учебной сети с учетом необходимых потоков, условий эксплуатации и общих точек отказа;
- научиться оформлять техническое задание и эксплуатационные правила, согласовывать изменения данных, доступа, резервного копирования и восстановления.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ПК-3 Способен разрабатывать проектные решения по защите информации автоматизированных систем (в том числе в геоинформационных системах)

ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности

Знать:

ПК-3.1/Зн1 Нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности

ПК-3.1/Зн2 Методы безопасности веб-приложения от критических угроз безопасности

ПК-3.1/Зн3 Систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации

Уметь:

ПК-3.1/Ум1 Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности

ПК-3.1/Ум2 Выявлять и устранять потенциальные угрозы безопасности в веб-приложениях

ПК-3.1/Ум3 Обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей

Владеть:

ПК-3.1/Нв1 Методами анализа и оценки информации на предмет ее соответствия критериям отнесения к различным видам тайны и степеням конфиденциальности

ПК-3.1/Нв2 Навыками по применению нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации

ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты

Знать:

ПК-3.2/Зн1 Нормативные и методические документые, регламентирующие классификацию субъектов и объектов доступа

ПК-3.2/Зн2 Принципы и методы организационной защиты информации

ПК-3.2/Зн3 Методы атаки и различные методы предотвращения атак

Уметь:

ПК-3.2/Ум1 Определять объекты доступа, которые подлежат защите, на основании их функционального назначения и чувствительности информации

ПК-3.2/Ум2 Выполнять проверку цифровых подписей и других криптографических атрибутов сообщений

ПК-3.2/Ум3 Анализировать результаты верификации и выявлять случаи нарушения целостности или подлинности сообщения

Владеть:

ПК-3.2/Нв1 Навыками работы с системами управления доступом и средствами контроля доступа

ПК-3.2/Нв2 Навыками работы с криптографическими библиотеками и инструментами верификации

ПК-3.2/Нв3 Методиками обеспечения безопасности при обработке и верификации криптографических сообщений

ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации

Знать:

ПК-3.3/Зн1 Регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем

ПК-3.3/Зн2 Программные, технические и методические средства информационных технологий

Уметь:

ПК-3.3/Ум1 Разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности распределенных информационных систем

ПК-3.3/Ум2 Развертывать веб-приложения в безопасной среде и поддерживать безопасность веб-приложений

ПК-3.3/Ум3 Осуществлять разработку и проектирование информационных систем в соответствии с поставленной задачей

Владеть:

ПК-3.3/Нв1 Навыками разработки проектов нормативных документов, регламентирующих работу по защите информации в организации

ПК-3.3/Нв2 Методами анализа и формализации информационных процессов объекта и связей между ними

ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем)

Знать:

ПК-3.4/Зн1 Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем)

ПК-3.4/Зн3 Технологии проектирования и построения защищенных информационных систем

ПК-3.4/Зн4 Особенности архитектуры распределённых информационных систем и роли системного программного обеспечения в них

Уметь:

ПК-3.4/Ум1 Анализировать и выбирать оптимальную топологию и архитектуру сети с учетом требований и условий эксплуатации

ПК-3.4/Ум2 Выполнять настройку системного программного обеспечения с учетом требований информационной безопасности

Владеть:

ПК-3.4/Нв1 Навыками проектирования и построения локальных и глобальных компьютерных сетей с использованием современных технологий и оборудования

ПК-3.4/Нв2 Навыками работы с системным программным обеспечением различных платформ в распределённых ИС

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.В.06 «Архитектура защищенных автоматизированных систем» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 4.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
4 семестр	180	5	32	48	64	Экзамен (36)
Всего	180	5	32	48	64	36

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотнесенные с результатами освоения программы
Раздел 1. Основные понятия и классификация защищенных автоматизированных систем	**39**	**8**	**9**	**22**	ПК-3.1 ПК-3.2 ПК-3.3

Тема 1.1. Основные понятия и классификация защищенных автоматизированных систем	39	8	9	22	ПК-3.4
Раздел 2. Основы защиты информации в защищенных автоматизированных системах	**16**	**6**	**10**		ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4
Тема 2.1. Основы защиты информации в защищенных автоматизированных системах	16	6	10		
Раздел 3. Основы организации разработки защищенных АС	**16**	**6**	**10**		ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4
Тема 3.1. Основы организации разработки защищенных АС	16	6	10		
Раздел 4. Общие принципы проектирования защищенных АС	**37**	**6**	**10**	**21**	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4
Тема 4.1. Общие принципы проектирования защищенных АС	37	6	10	21	
Раздел 5. Работа с данными в автоматизированных информационных системах	**36**	**6**	**9**	**21**	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4
Тема 5.1. Работа с данными в автоматизированных информационных системах	36	6	9	21	
Итого	**144**	**32**	**48**	**64**	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Основные понятия и классификация защищенных автоматизированных систем

Тема 1.1. Основные понятия и классификация защищенных автоматизированных систем

Классификация автоматизированных систем (АС). Информационные технологии, используемые в АС. Жизненный цикл АС. Основные угрозы безопасности информации в автоматизированных системах. Отказоустойчивость АС. Виды защищаемых сведений и правовые основания ограничения доступа. Персональные данные, коммерческая тайна и степени секретности государственной тайны; различие этих режимов. Субъекты и объекты доступа, внешние взаимодействия и условия эксплуатации.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 2. Основы защиты информации в защищенных автоматизированных системах

Тема 2.1. Основы защиты информации в защищенных автоматизированных системах

Понятия информации и информационных ресурсов. Предмет защиты информации. Объект защиты информации. Понятие информационной безопасности. Понятие политики информационной безопасности. Понятие системы защиты информации. Основные положения безопасности автоматизированных систем. Трехэтапная разработка мер по обеспечению безопасности автоматизированных систем. Стадия выработки требований. Стадия определения способов защиты. Стадия определения функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты. Основные принципы обеспечения информационной безопасности в автоматизированной системе (АС). Принципы, позволяющие реализовать положения по защите АС. Принцип системности. Принцип комплексности. Принцип непрерывной защиты. Минимальные привилегии, запрет по умолчанию, контроль обращений. Матрица ролей и операций, прямые и унаследованные права, регистрация событий. Связь организационных правил и технических механизмов.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 3. Основы организации разработки защищенных АС

Тема 3.1. Основы организации разработки защищенных АС

Последовательность и содержание этапов разработки АС. Методы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем. Методы и средства обеспечения отказоустойчивости автоматизированных систем. Критерии оценки защищенности АС. Методы обеспечения информационной безопасности АС. Организация коллективной разработки программного обеспечения АС. Стадии и результаты создания АС по ГОСТ Р 59793-2021. Согласование версий и проверка изменений. Условия приемки, испытания отказоустойчивости, различие доступности сервиса и сохранности последних данных.

Текущий контроль

Вид (форма) контроля
Практическая работа

Раздел 4. Общие принципы проектирования защищенных АС

Тема 4.1. Общие принципы проектирования защищенных АС

Проектирование защищенных АС. Методы проектирования. Содержание этапов проектирования. Основы ведения конструкторской документации. Структура и содержание технического задания. Построение комплексной защиты АС. Основы проектирования комплексной защиты информационной безопасности от НСД. Средства обеспечения надежности защищенных АС. Организация хранения информации в защищенных АС. Техническое задание по ГОСТ 34.602-2020. Сегменты сети, необходимые потоки, межсетевые экраны и защищенный межфилиальный обмен. Резервирование, общие зависимости и прослеживаемость требования до решения и проверки.

Текущий контроль

Вид (форма) контроля
Практическая работа

Раздел 5. Работа с данными в автоматизированных информационных системах

Тема 5.1. Работа с данными в автоматизированных информационных системах

Жизненный цикл АС. Порядок создания изделий ИТ, удовлетворяющих требованиям безопасности. Классификация новых наборов данных, управление эффективными правами, резервное копирование и проверка восстановления. Отличие репликации от сохранения предыдущих состояний. Согласование изменений данных, архитектуры, требований и эксплуатационных документов.

Текущий контроль

Вид (форма) контроля
Практическая работа

6. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Экзамен, 4 семестр.

Промежуточная аттестация по дисциплине проводится в форме экзамена. Конкретная форма проведения — компьютерное тестирование по теоретическому материалу или устное собеседование по вопросам билетов — утверждается кафедрой и доводится до сведения обучающихся не позднее чем за месяц до начала промежуточной аттестации. При компьютерном тестировании итоговый результат определяется как отношение количества набранных баллов к максимально возможному количеству баллов. При устном собеседовании билет включает вопросы из перечня вопросов; преподаватель вправе задать дополнительные и уточняющие вопросы.

Критерии оценивания при проведении промежуточной аттестации в форме компьютерного тестирования:

Экзамен оценивается по пятибалльной шкале:

- оценка «отлично» выставляется, если обучающийся набрал 86–100 баллов и продемонстрировал системное и полное освоение содержания дисциплины; ответы правильные, обоснованные и терминологически точные;
- оценка «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, если основное содержание освоено; допущены отдельные неточности, не влияющие на общее понимание материала;
- оценка «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если освоены базовые понятия и положения, но имеются существенные пробелы и ошибки;
- оценка «неудовлетворительно» выставляется, если обучающийся набрал 0–55 баллов; не освоен необходимый минимум содержания дисциплины; результаты обучения не достигнуты.

Критерии оценивания при проведении промежуточной аттестации в форме устного собеседования по билетам:

Экзамен оценивается по пятибалльной шкале:
- оценка «отлично» выставляется, если даны полные, правильные и логически последовательные ответы; терминология применяется корректно; приведены необходимые обоснования и примеры; дополнительные вопросы раскрыты;
- оценка «хорошо» выставляется обучающемуся, если вопросы раскрыты правильно и достаточно полно; отдельные неточности исправлены после уточняющих вопросов;
- оценка «удовлетворительно» выставляется обучающемуся, если основные положения раскрыты фрагментарно; имеются существенные неточности, однако базовое понимание продемонстрировано;
- оценка «неудовлетворительно» выставляется, если вопросы не раскрыты либо допущены принципиальные ошибки; отсутствует владение базовой терминологией.

7. Оценочные материалы текущего контроля

Раздел 1. Основные понятия и классификация защищенных автоматизированных систем
Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 1.1. Основные понятия и классификация защищенных автоматизированных систем

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Классификация сведений учебной системы

По описанию портала выделить карточки заявителей, обезличенные сводки и открытые справочники. Для каждого набора проверить, позволяет ли он прямо или косвенно определить человека, указать основание вывода и необходимые ограничения доступа. Не считать удаление имени достаточным обезличиванием, если другие поля сохраняют возможность идентификации.

2. Различение режимов и степеней секретности

Изучить статью 8 закона о государственной тайне и предоставленные преподавателем условные карточки с уже установленными правовыми основаниями ограничений. Разнести сведения по указанным режимам, назвать три степени секретности государственной тайны и объяснить, почему их грифы нельзя произвольно присваивать обычному закрытому документу организации.

3. Субъекты и объекты в модели угроз

По схеме учебной ГИС определить действующих пользователей и сервисы, защищаемые слои карты, файлы и учетные записи. Прочитать положения методики оценки угроз об объектах воздействия, затем для двух обращений явно указать субъект, объект, действие и возможное последствие нарушения.

4. Границы и жизненный цикл АС

Описать назначение учебной системы, ее пользователей, внешние взаимодействия и условия работы. По ГОСТ Р 59793-2021 выбрать состав стадий для учебного проекта и обозначить результаты, необходимые для перехода к проектированию и проверкам.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Расположите шаги описания угрозы: сначала определяют защищаемый объект, затем возможное воздействие, после этого последствие.

А. Описать воздействие
Б. Указать последствие
В. Выбрать объект

2. Упорядочьте проверку карточки: сначала прочитайте поля, затем установите связь с человеком, после этого сделайте вывод о наличии персональных данных.

А. Записать обоснованный вывод
Б. Проверить связь с определенным или определяемым человеком

В. Прочитать поля

3. В данном проекте обследование предшествует выбору концепции, а концепция служит основанием ТЗ. Укажите порядок.

А. Выбрать концепцию

Б. Разработать ТЗ

В. Обследовать объект

4. Упорядочьте разбор происшествия по заданной схеме: факт — затронутые данные — последствие.

А. Описать негативное последствие

Б. Записать наблюдаемый факт

В. Установить затронутые данные

5. Организация готовит учебный перечень коммерческой тайны. Сначала собирают сведения, затем проверяют критерии и законные ограничения, после этого составляют проект перечня.

А. Собрать описание сведений

Б. Составить обоснованный проект перечня

В. Проверить критерии и ограничения

6. В учебной проверке лишнее право сначала обнаруживают, затем обосновывают нужный доступ, после согласования меняют правило и проверяют результат.

А. Найти лишнее право

Б. Проверить разрешенную и запрещенную операции

В. Определить необходимый доступ

Г. Изменить правило после согласования

Раздел 2. Основы защиты информации в защищенных автоматизированных системах

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 2.1. Основы защиты информации в защищенных автоматизированных системах

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Права ролей на данные

В учебной СУБД создать или использовать роли читателя и редактора для тестовой таблицы. Назначить необходимые права, выполнить чтение и изменение от каждой роли, затем сравнить фактические решения с матрицей. Если используется готовый протокол стенда, восстановить по нему конфигурацию прав и найти расхождение.

2. Проект порядка обращения с закрытыми сведениями

Для вымышленной организации с коммерческой тайной подготовить фрагмент порядка: перечень сведений, предоставление и прекращение доступа, учет допущенных лиц и передача контрагенту. Сверить состав мер со статьей 10 закона № 98-ФЗ, показать связь организационного правила и технического ограничения.

3. Состав журнала контроля доступа

Для успешного чтения и отказа в изменении определить поля события. По небольшому учебному журналу восстановить, кто обращался к какому объекту и чем закончилась операция. Предложить правило доступа к самому журналу, исключив запись паролей и иных ненужных секретов.

4. От требования к механизму защиты

Взять сценарий несанкционированного изменения слоя карты и последовательно сформулировать требование, выбрать способ защиты, описать реализующие функции и процедуры. Для выбранного механизма указать короткую проверку и его ограничения.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Укажите порядок трех этапов разработки мер защиты, изучаемых в теме.

А. Определить способы защиты
Б. Определить функции, процедуры и средства защиты
В. Выработать требования

2. Упорядочьте настройку роли: нужные действия уже известны; сначала выбирают права, затем назначают их, после этого проверяют.

А. Назначить их роли
Б. Выбрать нужные права
В. Выполнить контрольные обращения

3. В учебном механизме сначала устанавливают субъект, затем запрашиваемое действие и объект, далее проверяют правило и выдают решение.

А. Разрешить или отклонить обращение
Б. Определить действие и объект
В. Проверить правило доступа
Г. Установить субъект

4. Упорядочьте анализ журнального события: сначала найдите запись, затем прочитайте субъект, объект и действие, после этого оцените результат.

А. Найти запись
Б. Оценить результат операции
В. Прочитать существенные поля

5. Для требования защиты сначала указывают желаемое поведение, затем условие проверки, после этого оценивают измеримость.

А. Задать условие проверки
Б. Проверить однозначность критерия
В. Описать поведение

6. После смены должности сначала выясняют новые обязанности, затем пересматривают права, после изменения проверяют фактический доступ.

А. Изменить согласованный набор прав
Б. Сопоставить с текущими правами
В. Определить новые обязанности
Г. Проверить фактический доступ

Раздел 3. Основы организации разработки защищенных АС

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 3.1. Основы организации разработки защищенных АС

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Проверяемые требования к разработке

Переработать три нечеткие формулировки из учебного описания: о доступе, времени выполнения операции и восстановлении. Для каждой задать условия, ожидаемый результат и способ проверки, не назначая произвольные нормативные числа.

2. Согласование коллективных изменений

Получить две версии схемы или конфигурации с противоречащими изменениями. Сравнить их, согласовать итоговый вариант и зафиксировать проверенную версию в учебном репозитории. Составить короткий порядок подачи, проверки и включения изменений.

3. Проверка отказоустойчивости

Для заданной пары основного и резервного узлов обозначить общие зависимости, задержку репликации и условия переключения. На изолированном стенде или по предоставленному протоколу исследовать отказ одного узла и объяснить, какие функции и данные сохранились.

4. Программа приемочной проверки

Для трех требований учебной АС подготовить фрагмент программы проверки: исходное состояние, действия, ожидаемый результат и запись факта. Одну проверку провести на стенде

или воспроизвести по исходному протоколу и оформить заключение.

Раздел 4. Общие принципы проектирования защищенных АС

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 4.1. Общие принципы проектирования защищенных АС

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Архитектура сети учебной ГИС

По условиям задачи разделить пользовательскую часть, прикладной сервис, базу и путь администрирования. Нарисовать схему размещения и потоков, выбрать подходящие соединения и ограничения, объяснить выбор с учетом нагрузки и внешних взаимодействий.

2. Реализация ограничений сетевого обмена

В учебной виртуальной сети настроить разрешенное соединение приложения с базой и запрет прямого соединения из пользовательского сегмента. Проверить оба маршрута доступа, сохранить конфигурацию и сопоставить фактический результат с архитектурной схемой.

3. Фрагмент технического задания

Подготовить для учебной АС цель, назначение, характеристику объекта и требования к структуре и доступу. Добавить порядок контроля выбранных требований и согласовать терминологию с архитектурной схемой по ГОСТ 34.602-2020.

4. Устранение общей точки отказа

На предложенной схеме найти один общий ресурс, отказ которого выводит из работы основной и резервный компоненты. Предложить изменение размещения или обеспечения ресурса, показать его на схеме и указать сценарий проверки результата.

Раздел 5. Работа с данными в автоматизированных информационных системах

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 5.1. Работа с данными в автоматизированных информационных системах

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Восстановление учебных данных

Создать резервную копию небольшой учебной базы, восстановить ее в отдельной среде и сравнить контрольные записи с исходными. Определить доступ к копии, ее расположение и соответствие заданной допустимой потере последних данных.

2. Отзыв эффективных прав

Для учебной роли с прямым разрешением и разрешением через группу выполнить последовательный отзыв прав. После каждого изменения проверить доступ, объяснить оставшиеся полномочия и подготовить полный набор действий для их прекращения.

3. Порядок выпуска изменения данных

Для добавления нового поля с закрытыми сведениями описать согласование требования, изменение схемы и прав, учебные проверки и решение о выпуске. Включить порядок действий при неуспешной проверке и связь с сохраненной исходной версией.

4. Согласование документации на новый набор данных

К имеющемуся проекту добавить условный набор карточек заявителей. Установить его классификационные признаки, обновить требования доступа, схему хранения и обмена и фрагмент порядка работы. Проверить отсутствие противоречий между документами.

8. Оценочные материалы промежуточной аттестации

4 семестр, Экзамен
Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4
Вопросы/Задания:

1. По какому признаку сведения относят к персональным данным?

2. Почему ценность информации сама по себе не означает установленный режим коммерческой тайны?

3. Чем государственная тайна отличается от произвольной внутренней отметки «закрыто»?

4. Что нужно назвать при описании угрозы для конкретного объекта АС?

5. Для чего проектировщику знать условия эксплуатации системы?

6. Как минимальные привилегии влияют на проектирование ролей?

7. Как связаны требования, способы и механизмы защиты?

8. Почему при отзыве доступа важно учитывать членство в группах?

9. Что должно позволять понять событие в журнале контроля доступа?

10. Как проверить правило «читатель не изменяет данные»?

11. Почему состав работ по созданию АС выбирают с учетом конкретного проекта?

12. Чем проверка общего результата отличается от простого хранения двух версий?

13. Какие сведения делают проверку требования воспроизводимой?

14. Почему асинхронное резервирование требует учитывать задержку передачи данных?

15. Какова роль приемочных испытаний в создании АС?

16. Чем назначение системы отличается от цели ее создания?

17. Что показывает схема потоков между сегментами сети?

18. Какие условия учитывать при выборе архитектуры сети для двух филиалов?

19. Что называют общей точкой отказа в рассматриваемой архитектуре?

20. Как обнаружить противоречие между ТЗ и архитектурной схемой?

21. Какая проверка подтверждает пригодность резервной копии?

22. Почему репликация не всегда защищает от ошибочного удаления?

23. Что такое эффективные права роли в учебной задаче?

24. Зачем защищать журнал событий от несанкционированного изменения?

25. Какие части проекта проверить при добавлении новых закрытых данных?

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Киренберг А. Г. Системное администрирование и информационная безопасность сетей ЭВМ: учебное пособие / А. Г. Киренберг. - Кемерово: КузГТУ имени Т.Ф. Горбачева, 2022. - 120 с. - 978-5-00137-292-9. - Текст: электронный // Издательство Лань: [сайт]. - URL: https://e.lanbook.com/book/257564 - Режим доступа: по подписке

2. Титова Л. Н. Информационная безопасность и защита информации: учебно-методическое пособие / Л. Н. Титова. - Уфа: БГПУ имени М. Акмуллы, 2013. - 108 с. - Текст: электронный // Издательство Лань: [сайт]. - URL: http://e.lanbook.com/books/element.php?pl1_id=56704 - Режим доступа: по подписке

3. Зобнин Ю. А. Разработка и внедрение автоматизированных информационных систем на предприятии: учебное пособие / Ю. А. Зобнин, А. С. Еропкина, О. В. Рындина. - Разработка и внедрение автоматизированных информационных систем на предприятии - Тюмень: Тюменский индустриальный университет, 2021. - 148 с. - 978-5-9961-2750-4. - Текст: электронный // IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/122402.html - Режим доступа: по подписке

Дополнительная литература

1. Ханипова Л. Ю. Информационная безопасность и защита информации / Л. Ю. Ханипова, Г. Р. Кутлова. - Уфа: БГПУ имени М. Акмуллы, 2010. - 112 с. - 978-5-87978-681-1. - Текст: электронный // Издательство Лань: [сайт]. - URL: http://e.lanbook.com/books/element.php?pl1_id=49513 - Режим доступа: по подписке

2. Информационная безопасность и защита информации / . - Самара: СамГУПС, 2012. - 150 с. - Текст: электронный // Издательство Лань: [сайт]. - URL: https://e.lanbook.com/book/130272 - Режим доступа: по подписке

9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

Не используются.

Ресурсы «Интернет»

1. https://scholar.google.ru/ - Гугл Академия
2. https://www.elibrary.ru/ - НЭБ eLIBRARY
3. https://intuit.ru/ - Электронная образовательная среда "ИНТУИТ"
4. https://e.lanbook.com/ - Электронная библиотечная система "Лань"
5. https://urait.ru - Образовательная платформа «Юрайт»

9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
1. Sublime Text 3;
2. 7Zip;
3. Microsoft Office;
4. Notepad++;
5. Microsoft Visual Studio;

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Не используется.

9.4. Оборудование и технические средства обучения

Компьютерный класс
- Маркерная доска - 0 шт.
- Моноблок - 64 шт.
- Проектор - 5 шт.
- Автоматизированное рабочее место (АРМ) - 15 шт.
- Доска настенная одноэлементная - 2 шт.

Учебная аудитория
- Автоматизированное рабочее место (АРМ) - 1 шт.
- Проектор - 2 шт.
- Доска настенная одноэлементная - 1 шт.

Смешанный тип
- Автоматизированное рабочее место (АРМ) - 1 шт.
- Доска настенная одноэлементная - 2 шт.
- Интерактивная панель - 1 шт.
- Проектор - 1 шт.

10. Методические указания по освоению дисциплины (модуля)

С целью успешного освоения данного предмета студенту необходимо выполнять домашние работы по указанным преподавателям темам и представленным на занятиях материалам. Для более успешного выполнения работы студенту предлагается использование учебно-методических материалов, соответствующих указанной теме.

Самостоятельная работа студентов описывается и регулируется методическими рекомендациями по дисциплине.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.