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
15 мая 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «Б1.О.04 ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ»

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): 2026

Срок получения образования: 2 года

Объем: в зачетных единицах: 10 з.е.
в академических часах: 360 ак.ч.

Москва, 2026

Разработчики:
Преподаватель кафедры Информационно-измерительных систем
Рябов В. С.

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	05.11.2025, № 12-25

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 и обосновывать защиту информационной системы: анализировать исходные условия, угрозы и слабые места, формулировать проверяемые требования, готовить техническое задание и согласованный технический проект, выбирать и проверять механизмы защиты с учетом эксплуатации и сопровождения.

Задачи изучения дисциплины:

- освоить основные требования и стандарты создания защищенных систем, анализа рисков и готовности к восстановлению;
- научиться планировать улучшение защиты и готовить структурированное техническое задание с наблюдаемыми критериями приемки;
- освоить функциональное моделирование и простые методы анализа данных для обоснования проектных решений;
- получить опыт применения и проверки средств защиты ОС, включая встроенные механизмы Astra Linux;
- освоить выбор и согласование виртуализированной среды, криптографических механизмов, облачных сервисов и ограниченного применения ИИ;
- научиться исследовать свойства реализации, обрабатывать недостатки и поддерживать согласованность требований, технического проекта и эксплуатационных процедур.

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

Компетенции, индикаторы и результаты обучения

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание

ОПК-1.1 Анализирует систему обеспечения информационной безопасности и формулирует требования по ее улучшению

Знать:

ОПК-1.1/Зн1 Содержание основных стандартов в области информационной безопасности

Уметь:

ОПК-1.1/Ум1 Организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения защиты информации в информационных системах

Владеть:

ОПК-1.1/Нв1 Анализировать сложные системы обеспечения информационной безопасности, выявляя их слабые места и области для улучшения

ОПК-1.2 Разрабатывает проект технического задания на создание системы обеспечения информационной безопасности

Знать:

ОПК-1.2/Зн1 Основные принципы классификации уязвимостей защиты по размещению данных в информационной системе

Уметь:

ОПК-1.2/Ум1 Применять современные программные инструментарии для моделирования угроз, анализа и оценки рисков информационной безопасности, а также использовать системы поддержки принятия решений при выборе эффективных проектов защиты

ОПК-1.2/Ум2 Применять эффективные методы управления безопасностью информационных систем

Владеть:

ОПК-1.2/Нв1 Разрабатывать комплексные и структурированные технические задания на создание систем обеспечения информационной безопасности, учитывая все аспекты проекта

ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности

ОПК-2.1 Разрабатывает технический проект системы (подсистемы, компоненты системы) обеспечения информационной безопасности в соответствии с техническим заданием, нормативно-правовой, организационно-распорядительной и методической документацией

Знать:

ОПК-2.1/Зн1 Методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения защиты информации в информационных система

Уметь:

ОПК-2.1/Ум1 Применять современные технологии моделирования и проектирования программных и программно-аппаратных систем

ОПК-2.1/Ум2 Подбирать меры и средства обеспечения информационной безопасности объекта защиты

ОПК-2.1/Ум3 Определять основные мероприятия по организации разработки системы защиты информации на объектах информатизации; разрабатывать технические проекты, документы, регламентирующие обеспечение информационной безопасности объектов информатизации (подсистемы либо компонента системы)

Владеть:

ОПК-2.1/Нв1 Разрабатывать комплексные технические проекты систем обеспечения информационной безопасности, интегрируя различные компоненты и подсистемы в единую архитектуру

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.О.04 «Защищенные информационные системы» относится к обязательной части образовательной программы и изучается в семестре(ах): 3, 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)

3 семестр	180	5	34	34	112	Зачет Курсовая работа
4 семестр	180	5	32	64	84	Зачет с оценкой
Всего	360	10	66	98	196	

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. Понятия и сущность защищённых автоматизированных систем	**22**	**6**	**4**	**12**	ОПК-1.1 ОПК-1.2 ОПК-2.1
Тема 1.1. Анализ и оценка информационных рисков, угроз и уязвимостей информационной системы. Аудит информационной безопасности	22	6	4	12	
Раздел 2. Общие принципы проектирования и разработки защищённых автоматизированных систем	**46**	**8**	**8**	**30**	ОПК-1.1 ОПК-1.2 ОПК-2.1
Тема 2.1. Сбор исходных данных об информационной системе. Разработка технического задания на создание системы защиты информации. Проектирование, внедрение, эксплуатация защищенных информационных систем	46	8	8	30	
Раздел 3. Основные технологии построения защищенных информационных систем	**46**	**8**	**8**	**30**	ОПК-1.1 ОПК-1.2 ОПК-2.1
Тема 3.1. Моделирование с помощью различных нотаций. IDEF – методологии	46	8	8	30	
Раздел 4. Защищенные ОС как основа построения защищенных информационных систем	**66**	**12**	**14**	**40**	ОПК-1.1 ОПК-1.2 ОПК-2.1

Тема 4.1. Базовые средства защиты современных ОС семейства Linux. Встроенные средства защиты информации на примере современных отечественных ОС (ОС Astra Linux)	66	12	14	40	
Раздел 5. Технологии виртуализации при построении защищенных информационных систем	**58**	**10**	**24**	**24**	ОПК-1.1 ОПК-1.2 ОПК-2.1
Тема 5.1. Технологии контейнерной виртуализации. Технологии виртуализации как средство обеспечения защиты при построении информационных систем. Интеграция встроенных средств защиты информации и технологий виртуализации на примере отечественных защищенных ОС (ОС Astra Linux)	58	10	24	24	
Раздел 6. Применение криптографических методов защиты информации при построении информационных систем	**54**	**10**	**24**	**20**	ОПК-1.1 ОПК-1.2 ОПК-2.1
Тема 6.1. Криптографические протоколы. Электронная цифровая подпись. Средства криптографической защиты информации	54	10	24	20	
Раздел 7. Перспективные направления в области проектирования защищенных информационных систем	**40**	**8**	**12**	**20**	ОПК-1.1 ОПК-1.2 ОПК-2.1
Тема 7.1. Применение облачных технологий при построении защищенных информационных систем	40	8	12	20	
Раздел 8. Средства разработки и тестирования защищенных информационных систем	**28**	**4**	**4**	**20**	ОПК-1.1 ОПК-1.2 ОПК-2.1
Тема 8.1. Верификация, статический анализ кода, динамический анализ, тестирование на проникновение	28	4	4	20	
Итого	**360**	**66**	**98**	**196**	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Понятия и сущность защищённых автоматизированных систем

Тема 1.1. Анализ и оценка информационных рисков, угроз и уязвимостей информационной системы. Аудит информационной безопасности

Основные понятия информационной безопасности. Защищенные информационные системы и требования к ним. Понятие, виды и структура информационных систем. Объекты защиты и угрозы безопасности в информационных системах. Комплексный подход к защите информации. Уровни формирования режима информационной безопасности: законодательный, административный, процедурный и программно-технический. Современная нормативная база в области создания защищенных информационных систем. ГОСТ Р ИСО/МЭК 27031-2012. ГОСТ Р 51583-2014. Анализ и оценка информационных рисков, угроз и уязвимостей информационной системы. Аудит информационной безопасности. Различие угрозы, уязвимости и последствий; качественная учебная оценка риска и пределы ее обоснования. Готовность к восстановлению критических услуг, общие зависимости, проверяемые свидетельства аудита.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 2. Общие принципы проектирования и разработки защищённых автоматизированных систем

Тема 2.1. Сбор исходных данных об информационной системе. Разработка технического задания на создание системы защиты информации. Проектирование, внедрение, эксплуатация защищенных информационных систем

Стадии и этапы разработки автоматизированных систем. Организация работ, функции заказчиков и разработчиков. Жизненный цикл информационной системы. Модели жизненного цикла. Сбор исходных данных об информационной системе. Требования к архитектуре информационных систем для обеспечения безопасности ее функционирования. Разработка технического задания на создание системы защиты информации. Проектирование, внедрение, эксплуатация защищенных информационных систем. Проверяемость требований, связь с угрозами и критериями приемки. Согласование изменения ТЗ, совместимость компонентов, подготовка эксплуатации и контроль результата модернизации. ГОСТ 34.602-2020 и ГОСТ Р 59793-2021 применяются с учетом предмета проекта.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 3. Основные технологии построения защищенных информационных систем

Тема 3.1. Моделирование с помощью различных нотаций. IDEF – методологии

Моделирование с помощью различных нотаций. Специальные методы моделирования, используемые при построении защищенных систем обработки информации. Описание модели безопасности. IDEF – методологии. Технология Data Mining, как процесс поддержки принятия решений, при построении защищенных систем обработки информации. Организационные и технические методы защиты информации. Основные подсистемы систем защиты информации, современное представление и реализация. IDEF0: цель, точка зрения, контекст, вход, выход, управление, механизм и согласованная декомпозиция. Аналитика событий как поддержка решения: подготовка данных, обучение и независимая проверка, ограничения переноса вывода.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 4. Защищенные ОС как основа построения защищенных информационных систем

Тема 4.1. Базовые средства защиты современных ОС семейства Linux. Встроенные средства защиты информации на примере современных отечественных ОС (ОС Astra Linux)

Основные методы и средства обеспечения защиты ОС. Базовые средства защиты современных ОС семейства Linux. Технологии обеспечения безопасности других ОС (Windows, MacOS) Проектирование, внедрение и эксплуатация наложенных средств защиты информации. Встроенные средства защиты информации на примере современных отечественных ОС (ОС Astra Linux). Учетные записи, группы, служебные процессы и минимальные привилегии. Совместное действие дискреционных и мандатных механизмов, проверка настроек и сохранение рабочих функций. Состав, защита и рассмотрение журналов.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 5. Технологии виртуализации при построении защищенных информационных систем

Тема 5.1. Технологии контейнерной виртуализации. Технологии виртуализации как средство обеспечения защиты при построении информационных систем. Интеграция встроенных средств защиты информации и технологий виртуализации на примере отечественных защищенных ОС (ОС Astra Linux)

Современные технологии программной и аппаратной виртуализации. Технологии контейнерной виртуализации. Технологии виртуализации как средство обеспечения защиты при построении информационных систем. Интеграция встроенных средств защиты информации и технологий виртуализации на примере отечественных защищенных ОС (ОС Astra Linux). Гостевое и общее ядро, пространства имен, лимиты ресурсов, capabilities и режим без привилегий root. Подключения каталогов, управление средой и ограничения изоляции. Сопровождение хоста и согласованная проверка конфигурации.

Текущий контроль

Вид (форма) контроля
Практическая работа

Раздел 6. Применение криптографических методов защиты информации при построении информационных систем

Тема 6.1. Криптографические протоколы. Электронная цифровая подпись. Средства криптографической защиты информации

Классификация криптографических алгоритмов. Основные направления и цели использования криптографических методов. Криптографические протоколы. Электронная цифровая подпись. Требования к средствам криптографической защиты информации. Примеры средств криптографической защиты информации. Различие шифрования, хеширования и подписи; симметричные и асимметричные ключи, установление доверия и прекращение использования скомпрометированного ключа. Границы TLS и проверка подлинности сервера. В современной терминологии применяется понятие электронной подписи; техническая проверка не означает автоматически юридическую квалификацию подписи.

Текущий контроль

Вид (форма) контроля
Практическая работа

Раздел 7. Перспективные направления в области проектирования защищенных информационных систем

Тема 7.1. Применение облачных технологий при построении защищенных информационных систем

Применение облачных технологий при построении защищенных информационных систем. Применение технологий искусственного интеллекта при проектировании и эксплуатации защищенных информационных систем. Разделение ответственности IaaS, PaaS и SaaS; управление данными и полномочиями организации. Недоверенные документы, предложения БЯМ и действия прикладных сервисов; проверка формата, смысла и прав вне модели, поведение при отказе.

Текущий контроль

Вид (форма) контроля
Практическая работа

Раздел 8. Средства разработки и тестирования защищенных информационных систем

Тема 8.1. Верификация, статический анализ кода, динамический анализ, тестирование на проникновение

Изучение государственных стандартов, содержащих требования, устанавливаемые российским законодательством к средствам разработки и тестированию программного обеспечения. Разработка безопасного программного обеспечения. Основные технологии обеспечения доверия к разрабатываемым средствам защиты информации. Верификация, статический анализ кода, динамический анализ, тестирование на проникновение. ГОСТ Р 56939-2024: требования безопасности, состав версии, сборка и зависимости, управление недостатками, воспроизводимость и повторные проверки. Возможности и пределы статического, динамического, композиционного и функционального анализа; предупреждение и подтвержденный недостаток.

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: Зачет, 3 семестр.

Промежуточная аттестация по дисциплине проводится в форме зачета. Она может быть организована как компьютерное тестирование либо как устное собеседование по билетам. Билет включает два теоретических вопроса и одно простое практическое задание. Конкретная форма утверждается кафедрой и доводится до обучающихся в установленный срок.

Критерии оценивания при проведении промежуточной аттестации в форме компьютерного тестирования:

Зачет оценивается по двухбалльной шкале («зачтено/не зачтено»):

- зачтено выставляется, если обучающийся набрал 60–100 %; достигнут необходимый уровень: основные понятия поняты, типовая задача решена корректно и с учетом установленных ограничений;
- не зачтено выставляется, если обучающийся набрал 0–59 %; не достигнут необходимый уровень: имеются принципиальные ошибки в понятиях, последовательности действий или обосновании решения.

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

Зачет оценивается по двухбалльной шкале («зачтено/не зачтено»):

- зачтено выставляется, если ответ раскрывает основные положения вопросов билета; термины применены корректно, практическая задача решена допустимым способом, существенные ошибки отсутствуют;
- не зачтено выставляется, если ответ отсутствует либо содержит принципиальные ошибки; не раскрыты основные понятия, практическая задача не решена или предложено недопустимое действие.

Промежуточная аттестация: Курсовая работа, 3 семестр.

Примерная тематика курсовых работ определяется преподавателем.

Курсовая работа оценивается по пятибалльной шкале:

- оценка «отлично» выставляется, если обучающийся набрал 86–100 баллов; результаты достигнуты полно; решения корректны, обоснованы и воспроизводимы;
- оценка «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, если основные результаты достигнуты; есть отдельные неточности без искажения метода;
- оценка «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если

достигнут минимально достаточный результат; имеются неполнота и ошибки в деталях;
- оценка «неудовлетворительно» выставляется, если обучающийся набрал 0–55 баллов; обязательные результаты не подтверждены или решение неработоспособно.

Промежуточная аттестация: Зачет с оценкой, 4 семестр.
Промежуточная аттестация по дисциплине проводится в форме «дифференцированный зачет». 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:
Зачет оценивается по пятибалльной шкале:
- зачтено с оценкой «отлично» выставляется, если обучающийся набрал 86–100 баллов и продемонстрировал системное и полное освоение содержания дисциплины; ответы правильные, обоснованные и терминологически точные;
- зачтено с оценкой «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, в случае, если основное содержание освоено, но допущены отдельные неточности, не влияющие на общее понимание материала;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если освоены базовые понятия и положения, но имеются существенные пробелы и ошибки;
- не зачтено («не удовлетворительно») – 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:
Зачет оценивается по пятибалльной шкале:
- зачтено с оценкой «отлично» выставляется, если обучающийся набрал 86–100 баллов и дал полные, правильные и логически последовательные ответы; терминология применяется корректно, приведены необходимые обоснования и примеры, дополнительные вопросы раскрыты;
- зачтено с оценкой «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, если вопросы раскрыты правильно и достаточно полно, а отдельные неточности исправлены после уточняющих вопросов;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если основные положения раскрыты фрагментарно, имеются существенные неточности, однако базовое понимание продемонстрировано;
- не зачтено («не удовлетворительно») – если обучающийся набрал 0–55 баллов, вопросы не раскрыты либо допущены принципиальные ошибки, отсутствует владение базовой терминологией.

7. Оценочные материалы текущего контроля

Раздел 1. Понятия и сущность защищённых автоматизированных систем
Контролируемые ИДК: ОПК-1.1 ОПК-1.2 ОПК-2.1

Тема 1.1. Анализ и оценка информационных рисков, угроз и уязвимостей информационной системы. Аудит информационной безопасности

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Объекты защиты и недостатки учебной ИС

По описанию учебного портала составить схему данных, компонентов и внешних связей; выделить три слабых места при хранении, передаче или обработке данных. Для каждого связать уязвимость, возможное воздействие и последствие, указать применимый источник требований.

2. Оценка риска и проверка исходных предположений

В доступном средстве моделирования или поддержки решений зафиксировать три риска и сравнить два варианта их обработки по явно заданным критериям. Показать, на каких исходных фактах основаны оценки, какие данные требуют проверки и как изменится выбор при изменении одного условия. Подготовить небольшой план сбора свидетельств для подтверждения обнаруженного недостатка.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Восстановите заданный порядок подготовки к восстановлению: проверка выполняется после подготовки процедуры.

А. Проверить восстановление на учебном примере
Б. Подготовить процедуру и необходимые ресурсы
В. Установить требования к восстановлению услуги

2. Упорядочьте уточнение угрозы при появлении нового внешнего подключения.

А. Рассмотреть возможное воздействие через подключение
Б. Уточнить сценарий угрозы и его последствия
В. Зафиксировать новое подключение и доступные данные

3. Упорядочьте получение обоснованного обнаружения аудита; критерий определяют до оценки свидетельств.

А. Сопоставить свидетельства с критерием и сформулировать обнаружение
Б. Определить проверяемое требование
В. Собрать и проверить относящиеся к нему свидетельства

Раздел 2. Общие принципы проектирования и разработки защищённых автоматизированных систем

Контролируемые ИДК: ОПК-1.1 ОПК-1.2 ОПК-2.1

Тема 2.1. Сбор исходных данных об информационной системе. Разработка технического задания на создание системы защиты информации. Проектирование, внедрение, эксплуатация защищенных информационных систем

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Организация работ по улучшению защиты

Для одного выявленного недостатка составить план модернизации: исходное состояние, требуемый результат, работы, ответственные роли, зависимости и способ контроля. Показать, что должно быть проверено до изменения рабочей среды и как организован возврат при неуспехе.

2. Техническое задание на систему защиты

Подготовить связный учебный проект ТЗ: основания, назначение и цели, характеристика объекта, требования, состав работ, контроль и приемка, подготовка объекта, документирование и источники разработки. Для требований указать условия и наблюдаемые признаки выполнения; проверить согласованность с исходной моделью угроз.

3. Технический проект подсистемы защиты

На основе учебного ТЗ выбрать компоненты защиты и описать их взаимодействие, данные, интерфейсы, настройки и организационные процедуры. Сопоставить решения с

требованиями, проверить совместимость компонентов и определить документы, необходимые для внедрения и эксплуатации.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте подготовку проверяемого требования: условия формулируют до критерия приемки.

А. Определить защищаемую операцию
Б. Указать наблюдаемый признак выполнения требования
В. Описать требуемое поведение в заданных условиях

2. Упорядочьте ввод учебной подсистемы: эксплуатация начинается после предусмотренной приемки.

А. Подготовить подсистему и документацию
Б. Передать подсистему в эксплуатацию
В. Провести предусмотренные испытания и приемку

3. Упорядочьте согласование изменения ТЗ; новое решение реализуют после согласования.

А. Реализовать согласованную редакцию требований
Б. Согласовать изменение с уполномоченными участниками
В. Описать предлагаемое изменение и его влияние

Раздел 3. Основные технологии построения защищенных информационных систем

Контролируемые ИДК: ОПК-1.1 ОПК-1.2 ОПК-2.1

Тема 3.1. Моделирование с помощью различных нотаций. IDEF – методологии

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Функциональная модель защищаемого процесса

Построить контекстную диаграмму IDEF0 одного учебного процесса и декомпозицию выбранной функции. Указать входы, выходы, управления, механизмы, цель и точку зрения; сопоставить граничные потоки двух уровней и пояснить место правил защиты.

2. Аналитика событий как поддержка решения

На небольшом искусственном наборе событий построить простую модель или правило выделения подозрительных обращений. Разделить данные для настройки и итоговой проверки, сохранить параметры преобразования признаков и сравнить прогнозы с известными метками. Объяснить ошибки и пределы применения результата к другой системе.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте устранение несовместимости двух средств защиты: повторная проверка следует за корректировкой.

А. Скорректировать согласованные настройки
Б. Воспроизвести конфликт средств на стенде
В. Повторно проверить совместную работу и защитные функции

2. Упорядочьте подготовку функциональной модели: детализация следует за определением границ.

А. Построить контекстное описание
Б. Установить цель и границы модели
В. Детализировать выбранную функцию

3. Восстановите порядок согласования термина на диаграмме: метки исправляют после согласования значения.

А. Привести метки диаграмм к согласованному значению
Б. Найти неоднозначный термин
В. Согласовать его значение в глоссарии

4. Упорядочьте честную оценку модели: тестовые данные не участвуют в обучении.

А. Оценить результат на отложенной тестовой части

Б. Обучить модель только на обучающей части

В. Разделить данные на обучающую и тестовую части

5. Упорядочьте исправление дочерней диаграммы, потерявшей внешний выход родительской функции.

А. Проверить согласованность уровней модели

Б. Сопоставить интерфейсы родительской и дочерней диаграмм

В. Восстановить отсутствующую связь результата с внешним выходом

Раздел 4. Защищенные ОС как основа построения защищенных информационных систем

Контролируемые ИДК: ОПК-1.1 ОПК-1.2 ОПК-2.1

Тема 4.1. Базовые средства защиты современных ОС семейства Linux. Встроенные средства защиты информации на примере современных отечественных ОС (ОС Astra Linux)

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Разграничение доступа средствами ОС

На учебной Linux-системе создать служебную и пользовательские учетные записи, организовать доступ через группу к рабочему каталогу и отделить чтение от изменения. Проверить права в актуальных сеансах и обосновать минимальные полномочия служебного процесса.

2. Интеграция встроенной защиты Astra Linux

На выделенном учебном стенде сопоставить заданную политику с действующими дискреционными и мандатными настройками Astra Linux. Разобрать разрешенную и запрещенную операции, объяснить совместное действие механизмов; предложить и проверить исправление одной неверной настройки без отмены требуемой политики.

3. Регистрация и рассмотрение событий защиты

Настроить или исследовать учебный журнал успешного и запрещенного доступа. Проверить наличие времени, субъекта, объекта, результата и связи событий одного обращения; подготовить порядок рассмотрения отказов и защиты самого журнала, исключив запись секретов.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте предоставление совместного доступа через новую группу: проверка выполняется после настройки.

А. Проверить доступ в сеансе с актуальным составом групп

Б. Создать группу и включить нужную учетную запись

В. Назначить группе необходимые права на учебный каталог

Раздел 5. Технологии виртуализации при построении защищенных информационных систем

Контролируемые ИДК: ОПК-1.1 ОПК-1.2 ОПК-2.1

Тема 5.1. Технологии контейнерной виртуализации. Технологии виртуализации как средство обеспечения защиты при построении информационных систем. Интеграция встроенных средств защиты информации и технологий виртуализации на примере отечественных защищенных ОС (ОС Astra Linux)

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Сопоставление виртуальной машины и контейнера

Подготовить два варианта размещения учебного приложения: в ВМ и контейнере. Изобразить

гостевое и общее ядро, управление средой, сеть и хранилище; сравнить границы изоляции и необходимые меры защиты для выбранной задачи. Один вариант реализовать на стенде.

2. Безопасные подключения данных контейнера

Разделить учебные каталоги на справочник для чтения и область записи отчетов. Настроить подключения и сетевые взаимодействия контейнера по нуждам приложения; проверить доступ к необходимым ресурсам и отсутствие доступа к постороннему каталогу. Указать, какие ограничения относятся к контейнеру, а какие задаются на хосте.

3. Проверка полномочий и ресурсов контейнерной среды

На учебном стенде сопоставить настройки приложения с реально нужными привилегиями, задать ограничение ресурсов и закрыть ненужный доступ к управлению средой. Провести небольшой ограниченный опыт, проверить рабочую функцию и подготовить порядок изменения образа и настроек.

Раздел 6. Применение криптографических методов защиты информации при построении информационных систем

Контролируемые ИДК: ОПК-1.1 ОПК-1.2 ОПК-2.1

Тема 6.1. Криптографические протоколы. Электронная цифровая подпись. Средства криптографической защиты информации

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Шифрование учебного файла и обращение с ключом

Используя доступное учебное средство, зашифровать искусственный файл и проверить восстановление его содержимого с правильным ключом. Разделить хранение шифртекста и ключевого материала, описать допустимых участников и порядок обращения с ключом; не использовать реальные секреты.

2. Проверка электронной подписи

Создать и проверить подпись искусственного документа в учебной среде. Повторить проверку после изменения документа и с другим открытым ключом; объяснить необходимость доверенной связи ключа с подписантом и отличие подписи от шифрования.

3. Границы защищенного соединения

На учебной схеме клиента, промежуточного узла и сервиса обозначить окончания TLS-соединений. Проверить соединение с доверенным сервером и отказ при нарушении проверки подлинности; определить защиту каждого участка и согласовать схему с требованиями доступа к данным.

Раздел 7. Перспективные направления в области проектирования защищенных информационных систем

Контролируемые ИДК: ОПК-1.1 ОПК-1.2 ОПК-2.1

Тема 7.1. Применение облачных технологий при построении защищенных информационных систем

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Распределение ответственности в облачной системе

Для выбранного учебного сервиса сопоставить варианты IaaS, PaaS и SaaS по управлению ОС, приложением, данными и учетными записями. Для одного варианта составить матрицу ответственности и перечень настроек, которые должна выполнить организация; условия договора обозначить как исходные данные, а не выдумывать.

2. Безопасное использование БЯМ в учебном процессе ИС

Выбрать короткую операцию обработки документа с помощью БЯМ и изобразить границы данных, предложения модели и прикладного действия. Подготовить обычный пример и

пример с недоверенной инструкцией в документе; проверить внешние ограничения полномочий и результата. Описать отказ от выполнения недопустимого действия и работу при недоступности модели.

Раздел 8. Средства разработки и тестирования защищенных информационных систем
Контролируемые ИДК: ОПК-1.1 ОПК-1.2 ОПК-2.1

Тема 8.1. Верификация, статический анализ кода, динамический анализ, тестирование на проникновение

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Сопоставление методов проверки безопасного ПО

Для небольшой учебной программы выбрать статический анализ, проверку поведения при исполнении и функциональные тесты. Зафиксировать состав версии и условия, выполнить доступные проверки, различить предупреждение инструмента и подтвержденный недостаток; связать каждый результат с проверяемым требованием.

2. Согласование исправления и технического проекта

На основе обнаруженного недостатка обновить требования, техническое решение и эксплуатационную процедуру. Показать изменение состава версии, повторить проверку исправления и связанных функций; подготовить согласованный комплект ТЗ, проекта и подтверждающих материалов для учебной приемки.

8. Оценочные материалы промежуточной аттестации

3 семестр, Зачет
Контролируемые ИДК: ОПК-1.1 ОПК-2.1 ОПК-1.2
Вопросы/Задания:

1. Чем уязвимость отличается от сценария угрозы?

2. Для чего устанавливают критерии оценки риска?

3. Почему вывод аудита должен иметь проверяемые свидетельства?

4. Чем восстановление данных отличается от восстановления услуги?

5. Что делает требование ТЗ проверяемым?

6. Какие результаты нужны до передачи подсистемы в эксплуатацию?

7. Почему средства защиты нужно проверять на совместимость?

8. Как согласовывается изменение требований?

9. Чем название продукта отличается от требования к защите?

10. Какие четыре вида связей описывает функциональный блок IDEF0?

11. Зачем перед моделированием определять цель и точку зрения?

12. Как проверяется согласованность декомпозиции?

13. Почему тестовая выборка не должна участвовать в настройке модели?

14. Почему схема защиты требует проверки реализации?

15. Какова роль групп в управлении файловыми правами Linux?

16. Почему нужно учитывать несколько действующих механизмов доступа Astra Linux?

17. Зачем служебной учетной записи минимальные полномочия?

18. Как отличить полезный журнал от избыточного сбора секретов?

19. Что проверяют после изменения настройки защиты ОС?

3 семестр, Курсовая работа
Контролируемые ИДК: ОПК-1.1 ОПК-2.1 ОПК-1.2
Вопросы/Задания:

1. Проект подсистемы выдачи доступа по согласованной заявке.

2. Проект прекращения доступа при завершении трудовых отношений.

3. Проект пересмотра полномочий при переводе сотрудника.

4. Проект управления временным доступом подрядчика.

5. Проект разделения обязанностей при утверждении платежной заявки.

6. Проект ограниченной служебной учетной записи резервирования.

7. Проект аварийного административного доступа.

8. Проект восстановления доступа пользователя.

9. Проект периодической проверки накопленных привилегий.

10. Проект совместного файлового пространства нескольких подразделений.

11. Проект защищенного сбора журналов от нескольких компонентов.

12. Проект ограничения изменения записей аудита.

13. Проект рассмотрения повторяющихся отказов доступа.

14. Проект согласования временных отметок событий.

15. Проект минимизации чувствительных сведений в журналировании.

16. Проект обработки заявки на изменение настройки защиты.

17. Проект учета и устранения слабых мест защищаемой ИС.

18. Проект согласованного обновления ОС нескольких рабочих мест.

19. Проект контролируемого вывода учебного сервера из эксплуатации.

20. Проект документирования действующей конфигурации защиты.

21. Проект восстановления критической пользовательской функции.

22. Проект устранения общей точки отказа защитной подсистемы.

23. Проект резервирования рабочего места дежурного оператора.

24. Проект защиты архива завершенных обращений.

25. Проект публикации разрешенной части внутреннего набора данных.

26. Проект обмена документами между подразделениями с разными правами.

27. Проект изолированного учебного стенда для проверки настроек защиты.

28. Проект совместимости встроенного и дополнительного средства защиты.

29. Проект защиты сервиса массовой подготовки отчетов.

30. Проект минимального набора системных служб рабочего сервера.

4 семестр, Зачет с оценкой
Контролируемые ИДК: ОПК-1.1 ОПК-2.1 ОПК-1.2
Вопросы/Задания:

1. Как различаются цели шифрования и подписи?

2. Какие условия нужны для доверенной проверки подписи?

3. Почему обычный хеш не всегда подтверждает отсутствие злонамеренной подмены?

4. Как определяются границы защиты TLS?

5. Почему управление ключами является частью защиты?

6. Как меняются обязанности при IaaS, PaaS и SaaS?

7. Что нужно выяснить до переноса данных в облачный сервис?

8. Почему внешний документ не должен менять правила приложения с БЯМ?

9. Какие проверки нужны между предложением модели и действием?

10. Как ограничить вывод по нескольким успешным проверкам БЯМ?

11. Чем различаются статический и динамический анализ?

12. Что подтверждает функциональное тестирование?

13. Зачем фиксировать состав сборки и зависимостей?

14. Как обрабатывают предупреждение анализатора?

15. Что проверяют после исправления недостатка?

16. Чем различаются ядра ВМ и обычного контейнера Linux?

17. Какую роль играют лимиты ресурсов?

18. Почему доступ к управлению контейнерами требует особого ограничения?

19. Как разграничить справочник и выходные файлы приложения?

20. Почему контейнер не заменяет сопровождение хоста?

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. 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

2. Защита компьютерной информации: учебное пособие / Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский, О. В. Скулябина. - Санкт-Петербург: БГТУ "Военмех" им. Д.Ф. Устинова, 2019. - 146 с. - 978-5-907054-82-0. - Текст: электронный // Издательство Лань: [сайт]. - URL: https://e.lanbook.com/book/157086 - Режим доступа: по подписке

3. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. - Защита компьютерной информации. Эффективные методы и средства - Саратов: Профобразование, 2024. - 543 с. - 978-5-4488-0074-0. - Текст: электронный // IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/145909.html - Режим доступа: по подписке

Дополнительная литература

1. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений / П.Н. Девянин. - Издательский центр "Академия", 2005. - 144 - 5-7695-2053-1. - Текст: непосредственный.

2. Богульская Н. А. Модели безопасности компьютерных систем: учебное пособие / Н. А. Богульская, М. М. Кучеров. - Красноярск: СФУ, 2019. - 206 с. - 978-5-7638-4008-7. - Текст: электронный // Издательство Лань: [сайт]. - URL: https://e.lanbook.com/book/157578 - 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://www.elibrary.ru/ - НЭБ eLIBRARY
2. https://e.lanbook.com/ - Электронная библиотечная система "Лань"
3. https://intuit.ru/ - Электронная образовательная среда "ИНТУИТ"
4. https://urait.ru - Образовательная платформа «Юрайт»
5. https://rusneb.ru/ - Национальная электронная библиотека (НЭБ)

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
Автоматизированное рабочее место (АРМ) - 15 шт.
Доска настенная одноэлементная - 2 шт.
Проектор - 1 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.