Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

**Программно-аппаратные средства защиты информации**

по направлению подготовки

**10.03.01 Информационная безопасность**

Направленность (профиль) подготовки:
**Безопасность компьютерных систем**

Форма обучения
**Очная**

Квалификация
**Бакалавр**

Год приема
**2025**

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2024

## 1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

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

ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.

ПК-1. Способен администрировать подсистемы защиты информации в операционных системах.

ПК-2. Способен проводить анализ эффективности программно-аппаратных средств защиты информации в операционных системах.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-1.2.1 Понимает принципы построения и функционирования операционных систем и компьютерных сетей.

ИОПК-1.2.2 Обладает знанием и демонстрирует навыки применения базовых методов защиты информации в компьютерных системах и сетях.

ИОПК-1.2.3 Демонстрирует навыки администрирования средств защиты информации в компьютерных системах и сетях.

ИОПК-9.1 Обладает знанием и демонстрирует навыки применения методов и средств криптографической защиты информации.

ИОПК-9.2 Обладает знанием и демонстрирует навыки применения методов и средств защиты информации от утечки по техническим каналам.

ИОПК-12.1 Понимает принципы работы информационных систем, средств обеспечения защиты информации, методики построения моделей угроз безопасности информации.

ИОПК-12.2 Демонстрирует навыки формирования исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.

ИПК-1.1. Определяет состав применяемых программно-аппаратных средств защиты информации в операционных системах.

ИПК-1.2. Оценивает угрозы безопасности информации операционных систем.

ИПК-1.3. Противодействует угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем.

ИПК-2.1. Проводит мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах.

ИПК-2.2. Оценивает оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах.

## 2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

- лабораторные работы

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения лабораторных работ. При оценивании необходимо продемонстрировать достижение всех запланированных индикаторов достижения компетенций.

Типовые варианты заданий для лабораторных работ:

1. Лабораторная работа "Защитные механизмы ОС Windows". Цель: познакомиться с возможностями и приобрести навыки конфигурирования встроенных средств защиты информации ОС Windows.

Задание 1 «Механизмы защиты ОС Windows». Написать краткий обзор механизмов защиты ОС Windows: управление доступом, аутентификация, шифрование, сертификаты, межсетевое экранирование и др.

Задание 2 «Настройка механизмом защиты ОС Windows»: настроить встроенные средств защиты информации ОС Windows: управление доступом, аутентификация, шифрование, межсетевое экранирование и др. При выполнении заданий рекомендуется использовать консоль управления mmc (Microsoft Management Console) с различными оснастками (групповая политика, шаблоны безопасности и др.).

После выполнения лабораторной работы составить в выложить в среду электронного обучения Мудл ТГУ отчет о проделанной работе, который включает в себя: название работы, ФИО и номер группы исполнителя работы, краткий обзор механизмов обеспечения информационной безопасности ОС Windows, скриншоты (снимки экрана) с реализованными настройками средств защиты информации.

2. Лабораторная работа "Защитные механизмы ОС Astra Linux". Цель: познакомиться с возможностями и приобрести навыки конфигурирования встроенных средств защиты информации ОС Astra Linux.

Задание 1 «Механизмы защиты ОС Astra Linux». Написать краткий обзор механизмов защиты ОС Astra Linux: дискреционный и мандатный механизмы разграничения доступа к файловым объектам, замкнутая программная среда и контроль целостности и др.

Задание 2 «Настройка механизмом защиты ОС Windows»: настроить встроенные средств защиты информации ОС Astra Linux: управление доступом, замкнутая программная среда и др.

После выполнения лабораторной работы составить в выложить в среду электронного обучения Мудл ТГУ отчет о проделанной работе, который включает в себя: название работы, ФИО и номер группы исполнителя работы, краткий обзор механизмов обеспечения информационной безопасности ОС Astra Linux, скриншоты (снимки экрана) с реализованными настройками средств защиты информации.

Типовые варианты тем лабораторных работ:

1. Установка и настройка СЗИ ViPNet Administrator.
   Создание структуры защищенной сети.
2. Настройка резервного копирования данных и восстановление данных.
3. Настройка политик безопасности в СЗИ ViPNet PolicyManager.
4. Установка и настройка СЗИ ViPNet Coordinator. Межсетевой шлюз.
5. Установка и настройка СЗИ ViPNetClient 4. Персональный сетевой экран.
6. Установка и настройка криптопровайдера ViPNetCSP.
7. Установка и настройка СЗИ «Соболь». Настройка общих параметров.
8. Установка и настройка СЗИ «Secret Net Studio». Управление устройствами.
9. Установка и настройка СЗИ «Secret Net Studio». Разграничение доступа.
10. Установка и настройка СЗИ «Secret Net Studio». Замкнутая программная среда.
11. Установка и настройка СЗИ «Secret Net Studio». Шифрование файлов.

Выполнение лабораторной работы задания оценивается в 100 баллов:

0-20 Студент не разбирается в задаче, не знает методов решения, не отвечает, либо отвечает, но с грубыми ошибками на вопросы преподавателя.

21-40 Студент слабо разбирается в задаче, плохо знает методы решения, не отвечает, либо отвечает, но с ошибками на вопросы преподавателя.

41-60 Студент в целом удовлетворительно разбирается в задаче, использует методы решения при подсказке преподавателя, отвечает на вопросы неуверенно, но с негрубыми ошибками. Представляет лабораторную работу на защите удовлетворительно.

61-80 Студент в целом уверенно разбирается в задаче, знает и использует методы решения практически самостоятельно, отвечает на вопросы с замечаниями. Представляет лабораторную работу на защите в целом хорошо, с замечаниями.

81-100 Студент отлично разбирается в задаче, знает и использует методы решения самостоятельно, отвечает на вопросы уверенно. Представляет лабораторную работу на защите отлично, уверенно.

Допуском до зачета с оценкой является выполнение 80% лабораторных работ с оценкой за каждую не менее 50 баллов.

**3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания**

Промежуточная аттестация осуществляется на основе выполнения студентом лабораторных работ и по результатам собеседования с использованием перечня контрольных вопросов по курсу. Вопросы выявляют все запланированные индикаторы достижения компетенций.

Примерный перечень контрольных вопросов по дисциплине:

1. Компьютерная система (КС) как объект защиты информации.
2. Понятие угрозы информационной безопасности в КС.
3. Классификация и общий анализ угроз информационной безопасности в КС.
4. Разработка политики информационной безопасности КС.
5. Методология политики безопасности компьютерных систем.
6. Основные положения политики информационной безопасности КС.
7. Жизненный цикл политики безопасности КС.
8. Функциональная модель системы защиты.
9. Понятие доступа и монитора безопасности.
10. Методология проектирования гарантированно защищенных КС.
11. Метод генерации изолированной программной среды.
12. Идентификация и аутентификация.
13. Инфраструктура открытых ключей.
14. Сертификаты открытых ключей X.509
15. Защита информации в файловой системе.
16. Шифрующая файловая система. Управление ключами.
17. Встроенные средства защиты информации операционных систем (ОС).
18. Возможности стандартных систем разграничения доступа ОС.
19. Принципы построения биометрических систем аутентификации.
20. Защита на уровне расширений BIOS.
21. Защита на уровне загрузчиков ОС.
22. Защита от программных закладок.

23. Контроль и управление доступом.
24. Персональные средства аутентификации.
25. Защита ПО с помощью электронных ключей.
26. Аппаратные модули безопасности.
27. Концепция доверенных сеансов связи.
28. Защищенные микрокомпьютеры.
29. Средства защиты виртуальной инфраструктуры.
30. Средства криптографической защиты информации.
31. Защита от вредоносного программного обеспечения.
32. Защита при передаче данных по каналу связи.
33. Предотвращение утечек информации.
34. Обнаружение и предотвращение вторжений.
35. Руководящие документы ФСТЭК России.
36. Модель угроз безопасности информации.
37. Сертификация автоматизированных систем.
38. Показатели защищенности от несанкционированного доступа к информации.

Критерии оценивания промежуточной аттестации:

Зачет с оценкой “отлично” по дисциплине проставляется, когда студент в совершенстве овладел материалом по всем разделам лекционного курса, а также показал требуемые умения и навыки при выполнении *всех* лабораторных работ.

Зачет с оценкой “хорошо” по дисциплине проставляется, когда студент овладел обязательным материалом по большинству разделов лекционного курса, возможно с некоторыми недостатками, а также показал требуемые умения и навыки при выполнении *большинства* лабораторных работ.

Зачет с оценкой “удовлетворительно” по дисциплине проставляется, когда студент овладел обязательным материалом по некоторым разделам лекционного курса, возможно с некоторыми недостатками, а также показал требуемые умения и навыки при выполнении *части* лабораторных работ.

Зачет с оценкой “неудовлетворительно” по дисциплине проставляется, когда студент имеет существенные пробелы по теоретическим разделам дисциплины и не показал требуемые умения и навыки при выполнении части лабораторных работ.

## 4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Примерный перечень контрольных вопросов для проверки остаточных знаний:

1. Компьютерная система (КС) как объект защиты информации.
2. Понятие угрозы информационной безопасности в КС.
3. Классификация и общий анализ угроз информационной безопасности в КС.
4. Разработка политики информационной безопасности КС.
5. Методология политики безопасности компьютерных систем.
6. Основные положения политики информационной безопасности КС.
7. Жизненный цикл политики безопасности КС.
8. Функциональная модель системы защиты.
9. Понятие доступа и монитора безопасности.
10. Методология проектирования гарантированно защищенных КС.
11. Метод генерации изолированной программной среды.
12. Идентификация и аутентификация.
13. Инфраструктура открытых ключей.
14. Защита информации в файловой системе.

15. Шифрующая файловая система. Управление ключами.
16. Встроенные средства защиты информации операционных систем (ОС).
17. Возможности стандартных систем разграничения доступа ОС.
18. Принципы построения биометрических систем аутентификации.
19. Защита на уровне расширений BIOS.
20. Защита на уровне загрузчиков ОС.
21. Защита от программных закладок.
22. Контроль и управление доступом.
23. Персональные средства аутентификации.
24. Защита ПО с помощью электронных ключей.
25. Средства защиты виртуальной инфраструктуры.
26. Средства криптографической защиты информации.
27. Защита от вредоносного программного обеспечения.
28. Защита при передаче данных по каналу связи.
29. Предотвращение утечек информации.
30. Обнаружение и предотвращение вторжений.

**5. Информация о разработчиках**

Тренькаев Вадим Николаевич, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности НИ ТГУ.