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

Информационная безопасность и работа с персональными данными

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Форма обучения
Очная

Квалификация
Магистр

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
А.Ю. Матросова

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 Способен решать актуальные задачи фундаментальной и прикладной математики.

ОПК-4 Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-1.1 Анализирует проблемы в области фундаментальной и прикладной математики.

ИОПК-1.2 Формулирует задачи исследования.

ИОПК-1.3 Решает актуальные задачи фундаментальной и прикладной математики.

ИОПК-4.2 Учитывает основные требования информационной безопасности.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

- тесты.

Пример типового теста (ИОПК-1.1.)

1. Связана ли информационная безопасность с защитой информационных ресурсов от разного рода угроз, способных нанести ущерб интересам личности или общества?
   a) Да
   b) Нет

2. Связана ли информационная безопасность с защитой информации от нежелательного разглашения, искажения, утраты или снижения степени доступности информации?
   а) Да
   б) Нет

3. Можно ли отнести к предметной области информационной безопасности следующее:
   а) классификация угроз безопасности информации
   б) способы, методы и средства защиты информации
   в) требования к защищенности информационных систем
   г) методология проектирования баз данных

4. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации называется
   а) правовой информацией
   б) защищаемой информацией

Ключи: 1 а), 2 а), 3 а) б) в), 4 б).

Критерии оценивания: тест считается пройденным, если обучающий ответил правильно как минимум на половину вопросов.

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

Промежуточная аттестация осуществляется на основе выполнения студентом лабораторных работ и/или по результатам собеседования с использованием перечня контрольных вопросов по курсу. Вопросы выявляют следующие индикаторы достижения компетенций: ИОПК-1.2, ИОПК-1.3.

Примерный перечень контрольных вопросов по курсу:

1. Термины, относящиеся к видам защиты информации.
2. Термины, относящиеся к способам защиты информации.
3. Термины, относящиеся к замыслу защиты информации.
4. Термины, относящиеся к объекту защиты информации.
5. Термины, относящиеся к угрозам безопасности информации.
6. Термины, относящиеся к технике защиты информации.
7. Несанкционированные операции с информацией.
8. Источники и классификация угроз безопасности информации.
9. Перечень типовых непреднамеренных искусственных угроз.
10. Перечень типовых преднамеренных искусственных угроз.
11. Классификация способов несанкционированного доступа.
12. Типовые атаки на коммуникационные протоколы.
13. Законодательные меры противодействия угрозам безопасности.
14. Организационные меры противодействия угрозам безопасности.
15. Физические и технические меры противодействия угрозам безопасности.
16. Аутентификация. Имитозащита. Цифровая подпись.
17. Симметричные шифры. Асимметричные шифры.
18. Криптографические протоколы.
19. Криптографические хеш-функции.
20. Классификация криптопротоколов.
21. Свойства цифровой подписи.
22. Криптографические протоколы аутентификации сообщений.
23. Криптографические протоколы идентификации.
24. Объект, субъект, доступ к информации, правила разграничения доступа.
25. Идентификация, аутентификация, авторизация.
26. Протоколирование и аудит (активный аудит).
27. Статистический метод обнаружения атак.
28. Сигнатурный метод обнаружения атак.
29. Дискреционное управление доступом.
30. Мандатное управление доступом.
31. Ролевое управление доступом.
32. Защита информации при хранении и передаче.
33. Защита от вредоносных программ.
34. Виды компьютерных вирусов и вредоносных программ.
35. Защита межсетевого взаимодействия.
36. Предотвращение утечек информации.
37. Аудит безопасности.

38. Угрозы корпоративной сети. Защита периметра сети.
39. Основные механизмы защиты корпоративной сети.
40. Средства защиты информации: межсетевые экраны.
41. Средства защиты информации: виртуальные частные сети.
42. Средства защиты информации: системы анализа защищенности.
43. Средства защиты информации: системы обнаружения атак.
44. Системы предотвращения утечки конфиденциальной информации.
45. Политика информационной безопасности организации.

Примеры лабораторных работ по курсу:

1. Лабораторная работа "OpenPGP / СКЗИ GnuPG". Цель: познакомиться со IETF-стандартом OpenPGP (документ RFC4880) и получить навыки работы со средством криптографической зашиты информации (СКЗИ) GnuPG (свободный некоммерческий вариант реализации стандарта OpenPGP). Задание 1 «Стандарт OpenPGP»: познакомиться со стандартом OpenPGP. Источники информации: слайды лекций, а также https://www.openpgp.org/about/standard. Задание 2 «СКЗИ GnuPG»: установить Gpg4win (www.gpg4win.org) – пакет GnuPG с набором утилит и расширений для работы в ОС Windows, далее создать и передать свой открытый ключ корреспонденту (абоненту) в обмен на его открытый ключ (для обмена ключами использовать социальную сеть, облачный сервис и т.п.), после чего проверить открытый ключ корреспондента через «отпечаток пальца», далее подписать (установить уровень доверия) открытый ключ корреспондента, после чего подписать и зашифровать сообщение и послать его корреспонденту, а также расшифровать и проверить подпись сообщения, которое прислал корреспондент, далее сформировать и проверить контрольную сумму для произвольного файла, измените файл и убедитесь, что СКЗИ GnuPG обнаруживает факт изменения. 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 стандарта OpenPGP, скриншоты выполненных действий с комментариями, в том числе сообщения от корреспондентов в зашифрованном и расшифрованном виде.

2. Лабораторная работа "Встроенные СЗИ ОС Windows". Цель: познакомиться с возможностями и приобрести навыки настройки встроенных средств защиты информации ОС Windows. Задание 1 «Обзор СЗИ ОС Windows». Написать краткий обзор механизмов и средств обеспечения информационной безопасности ОС Windows: управление доступом к ресурсам ОС, аутентификация, аудит, шифрование данных, сертификаты, межсетевое экранирование и др. Задание 2 «Настройка СЗИ ОС Windows». При выполнении заданий рекомендуется использовать консоль управления mmc (Microsoft Management Console) с различными оснастками (групповая политика, шаблоны безопасности и др.). Задача 1. Управление доступом (оснастка Локальные пользователи и группы): создать пользователей UserA и UserB, создать группу Students и настроить политику безопасности группы Students, приписать пользователей UserA и UserB к группе Students, настроить права доступа (частичный доступ) UserA к заданному каталогу (папке), настроить права доступа (полный доступ) UserB к заданному каталогу (папке), проверить выполнение ограничений прав доступа UserA и UserB. Задача 2. Аудит (протоколирование) (оснастка Редактор объектов групповой политики - Политика "Локальный компьютер"): установить аудит событий входа в систему (успех, отказ), открыть Журнал регистрации событий и определить последний вход в систему, установить аудит выбранного каталога (папки) для пользователя UserA, настроить параметры аудита, открыть Журнал безопасности и определить последние изменения отслеживаемого каталога (папки). Задача 3. Межсетевой

экран (брандмауэр) (оснастка Монитор брандмауэра): создать правило брандмауэра для входящего/исходящего подключения, проверить на практике выполнения ограничений созданных правил. Задача 4. Диспетчер сертификатов ОС Windows (оснастка Сертификаты): просмотреть сертификаты, установленные в ОС Windows, экспортировать произвольный сертификат, импортировать произвольный сертификат в папку Личные. Задача 5. Шаблон безопасности (оснастка Шаблоны безопасности): создать шаблон безопасности “Учебный” и реализовать рекомендуемую настройку Политики паролей, Политики блокировки учетной записи, Политики аудита, Параметры назначения прав пользователя. 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.

3. Лабораторная работа "Банк данных угроз безопасности информации ФСТЭК России"(www.bdu.fstec.ru). Цель: овладеть базовыми понятиями информационной безопасности и изучить существующие угрозы безопасности информации. Задание: используя Банк данных угроз безопасности информации ФСТЭК России, детально изучить три угрозы безопасности информации (описание угрозы, источники угрозы, объект воздействия, последствия реализации угрозы), присущих некоторому одному выбранному ИТ-объекту (облачная система, грид-система, виртуальная машина, беспроводная сеть, web-приложение, хранилище больших данных и т.п.), а также три устраненные уязвимости для некоторого одного выбранного Вами ПО (СУБД MySQL, браузер Google Chrome и т.п.). Также изучить термины по информационной безопасности: угроза, уязвимость, конфиденциальность, целостность, доступность (см. https://bdu.fstec.ru/terms). 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, результат выполнения работы, т.е. список определений следующих терминов: угроза, уязвимость, конфиденциальность, целостность, доступность, а также список изученных угроз и уязвимостей с их номерами (кодами).

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 (при оценивании необходимо продемонстрировать достижение **всех** запланированных индикаторов достижения компетенций):

1. Изложить основные понятия информационной безопасности (ИБ).
2. Описать законодательные методы обеспечения ИБ.
3. Описать административно-организационные методы обеспечения ИБ.
4. Сравнить симметричные и асимметричные шифры.
5. Предоставить схему гибридной (комбинированной) криптосистемы.
6. Предоставить схему электронной цифровой подписи.
7. Изложить метод обеспечения целостности сообщения.
8. Изложить основные свойства электронной цифровой подписи.
9. Охарактеризовать парольный метод аутентификации.
10. Охарактеризовать аутентификацию на базе протокола «запрос-ответ».
11. Перечислить цели и задачи протоколирования и аудита.
12. Охарактеризовать статистический метод обнаружения компьютерных атак.
13. Охарактеризовать сигнатурный метод обнаружения компьютерных атак.
14. Охарактеризовать дискреционное управление доступом.
15. Охарактеризовать мандатное управления доступом.
16. Охарактеризовать ролевое управление доступом.
17. Перечислить функции, которые может выполнять межсетевой экран.
18. Классифицировать компьютерные вирусы и вредоносные программы.
19. Изложить способы распространения и обнаружения вредоносных программ.
20. Изложить типовое содержание политики безопасности предприятия.
21. Охарактеризовать технологию построения виртуальных частных сетей.
22. Охарактеризовать технологию анализа защищенности сети.
23. Классифицировать системы обнаружения атак.
24. Изложить несанкционированные операции с информацией.
25. Классифицировать угрозы безопасности информации.
26. Перечислить типовые непреднамеренные искусственные угрозы.
27. Перечислить типовые преднамеренные искусственные угрозы.
28. Классифицировать способы несанкционированного доступа.
29. Перечислить типовые атаки на коммуникационные протоколы.
30. Охарактеризовать дискреционное управление доступом.
31. Охарактеризовать мандатное управление доступом.
32. Охарактеризовать ролевое управление доступом.

Информация о разработчиках

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