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

САЕ Институт «Умные материалы и технологии»

УТВЕРЖДАЮ:
Директор
_____И.А. Курзина
«05» _____11_____ 2024 г.

Оценочные материалы по дисциплине

Основы информационной безопасности

по направлению подготовки

19.03.01 Биотехнология

Направленность (профиль) подготовки:
«Молекулярная инженерия»

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
_____И.А. Курзина

Председатель УМК
_____Г.А. Воронова

Томск – 2024

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

Целью освоения дисциплины является формирование следующих компетенций:

УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

ОПК-2 Способен осуществлять поиск, хранение, обработку и анализ профессиональной информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий, включая проведение расчетов и моделирование, с учетом основных требований информационной безопасности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИУК-1.1 Осуществляет поиск информации, необходимой для решения задачи;

ИОПК-2.1 Проводит информационный поиск по тематике исследования и осуществляет критический анализ полученной информации.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– Реферат
– Опрос
– Лабораторные работы

2.1. Темы индивидуальных заданий (рефератов) (ИУК-1.1., ИОПК-2.1.)

Самостоятельная работа студентов по курсу «Основы информационной безопасности» завершается подготовкой доклада и написанием реферата по одной из выбранных тем. План работы и тема согласовываются с преподавателем.

Примерные темы для рефератов

1. Информация как предмет защиты;
2. Компьютерная система, как объект информационной безопасности;
3. Общая характеристика методов и средств защиты информации в компьютерных системах;
4. Виды информации, подлежащие защите. Государственная тайна;
5. Организационно-правовые аспекты защиты информации и авторского права;
6. Текущее состояние российского законодательства в области информационной безопасности;
7. Источники и носители защищаемой информации;
8. Современные атаки через Интернет на информационные ресурсы;
9. Вирусы и антивирусы. Классификация компьютерных вирусов. Методы обнаружения и удаления компьютерных вирусов;
10. Основные программные механизмы защиты информации;
11. Технические каналы утечки информации;
12. Основные технические механизмы защиты информации;
13. Межсетевые экраны;
14. Акустический канал утечки информации;
15. Характеристика оптических каналов утечки информации;

16. Радиоэлектронный канал утечки информации;
17. Исторический обзор криптографических методов защиты информации;
18. Методы шифрования информации. Электронная подпись;
19. Современные способы кодирования информации в вычислительной технике;
20. Облачные хранилища данных. Примеры различных серверов, особенности каждого из них;
21. Особенности корпоративных сетей ВУЗов;
22. Угрозы информационной безопасности ВУЗа и анализ рисков;
23. Наиболее востребованные компетенции специалиста по информационной безопасности.

Критерии оценивания:

Подготовка доклада по выбранной теме оценивается по шкале зачтено или не зачтено. Оцениваются полнота, точность и логичность изложения материала, а также знание теоретических сведений по тематике защищаемого реферата.

При проведении аттестации в форме зачета в конце семестра обучающемуся, успешно сдавшему реферат, дается три вопроса, в которых требуется по заданной теме дать определение ряда понятий, сформулировать ответы и проиллюстрировать их примерами.

2.2 Примеры вопросов для опроса (ИУК-1.1., ИОПК-2.1.)

1. Информация как предмет защиты;
2. Компьютерная система, как объект информационной безопасности;
3. Общая характеристика методов и средств защиты информации в компьютерных системах;
4. Виды информации, подлежащие защите. Государственная тайна;
5. Организационно-правовые аспекты защиты информации и авторского права;
6. Текущее состояние российского законодательства в области информационной безопасности;
7. Источники и носители защищаемой информации;
8. Современные атаки через Интернет на информационные ресурсы;
9. Вирусы и антивирусы. Классификация компьютерных вирусов. Методы обнаружения и удаления компьютерных вирусов;
10. Основные программные механизмы защиты информации;
11. Технические каналы утечки информации;
12. Основные технические механизмы защиты информации;
13. Межсетевые экраны;
14. Акустический канал утечки информации;
15. Характеристика оптических каналов утечки информации;
16. Радиоэлектронный канал утечки информации;
17. Исторический обзор криптографических методов защиты информации;
18. Методы шифрования информации. Электронная подпись;
19. Современные способы кодирования информации в вычислительной технике;
20. Облачные хранилища данных. Примеры различных серверов, особенности каждого из них;
21. Особенности корпоративных сетей ВУЗов;

22. Угрозы информационной безопасности ВУЗа и анализ рисков;
23. Наиболее востребованные компетенции специалиста по информационной безопасности.

Критерии оценивания:

Оценка	Критерии соответствия
зачтено	1) Студент выполнил индивидуальное задание, подготовил реферат по теме. Содержание реферата и ответы на вопросы являются полными, с пониманием терминологии предмета; 2) Успешно пройдены два теста в Moodle.
не зачтено	1) Не подготовлен реферат по выбранной теме. Студент не может логически связно отвечать на вопросы; 2) Успешно пройден один тест в Moodle.

2.3 Примеры лабораторных работ (ИУК-1.1., ИОПК-2.1.)

1. Лабораторная работа №1. Теоретические и практические основы облачного хранения данных.

Основная цель – научить студентов использовать облачные хранилища с соблюдением требований Инф.безопасности.

2. Лабораторная работа №2 Организация многопрофильного рабочего места.

Основная цель – научить студентов настраивать и использовать компьютеры общего доступа для работы с несколькими пользователями с учетом требований Инф.безопасности.

Оценка «зачтено» выставляется в случае, если студент верно выполнил все задания лабораторной работы.

Оценка «незачтено» выставляется в случае, если студент верно выполнил все задания лабораторной работы.

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

Промежуточная аттестация проводится в виде защиты реферата по согласованной с преподавателем теме, а также ответы на вопросы. Вопросы позволяют оценить уровень сформированности компетенций ИУК-1.1., ИОПК-2.1. в рамках изучаемых разделов, а подготовка доклада покажет, насколько студент владеет навыками публичного представления результатов работы по выбранной теме исследования.

При проведении аттестации в форме зачета в конце 1-го семестра обучающемуся успешно сдавшему реферат, дается три вопроса, в которых требуется по заданной теме дать определение ряда понятий, сформулировать ответы и проиллюстрировать их примерами.

Перечень контрольных вопросов:

1. Понятие информационной безопасности;
2. Основные составляющие информационной безопасности;
3. Собственник, владелец информации. Правила отнесения информации к защищаемой;
4. Что такое защита информации?
5. Что такое конфиденциальность?

6. Основные угрозы информационной безопасности. Классификация угроз;
7. Законодательный уровень информационной безопасности и почему он важен?
8. Законодательные акты в области информационной безопасности;
9. Какие сведения составляют государственную тайну?
10. Государственная тайна ее существенные признаки;
11. Порядок засекречивания информации, составляющей государственную тайну.
12. Основания для рассекречивания сведений, составляющих государственную тайну;
13. Национальные интересы РФ в информационной сфере и их обеспечение;
14. Источники угроз информационной безопасности РФ;
15. Сущность и особенности информационной войны;
16. Методы и приемы современных информационных войн;
17. Информационная война. Традиционные методы и новые тенденции;
18. Что такое персональные данные и почему они важны?
19. Способы защиты персональных данных;
20. Принципы защиты информации при передаче данных;
21. Защита информации на жестком диске;
22. Защита информации в локальных вычислительных сетях;
23. Проблема защиты информации в корпоративных сетях и почему она актуальна?
24. Понятие идентификации и аутентификации;
25. История появления компьютерного вируса;
26. Понятие вредоносной программы;
27. Классификация вредоносных программ;
28. Основные способы распространения вредоносных программ;
29. Основные организационные мероприятия, производимые для защиты от компьютерных вирусов;
30. Признаки заражения ПК вирусом. Выбор антивирусной программы.

«Зачет» ставится в том случае, если обучающийся подготовил доклад и ответил на два вопроса, а также успешно пройдены в течение семестра два теста в Moodle. В таблице 1 приведена система оценивания при проведении промежуточной аттестации.

Таблица 1. Система критериев при оценивании индивидуального задания (реферата)

Оценка	Критерии соответствия
зачтено	1) Студент выполнил индивидуальное задание - подготовил реферат по теме. Содержание реферата и ответы на вопросы являются полными, с пониманием терминологии предмета; 2) Успешно пройдены два теста в Moodle.
не зачтено	3) Не подготовлен реферат по выбранной теме. Студент не может логически связно отвечать на вопросы; 4) Успешно пройден один тест в Moodle.

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

Пример тестовых вопросов (ИУК-1.1; ИОПК-2.1.):

1. Какое из утверждений НЕ относится к принципам информационной безопасности?

* А. Конфиденциальность – защита информации от несанкционированного доступа.
* Б. Целостность – защита информации от несанкционированных изменений.
* В. Доступность – обеспечение доступа к информации только авторизованным пользователям.
* Г. Достоверность – гарантия того, что информация является подлинной и не является подделкой.

Ответ: В.

2. Какой тип атаки предполагает внедрение вредоносного кода в легитимное программное обеспечение?

* А. Фишинговая атака
* Б. DDoS-атака
* В. Троянская атака
* Г. SQL-инъекция

Ответ: В.

3. Что такое межсетевой экран (firewall) и какую функцию он выполняет?

* А. Программное обеспечение, которое анализирует трафик сети и блокирует вредоносный код.
* Б. Программное обеспечение, которое шифрует передаваемые данные, делая их недоступными для посторонних.
* В. Аппаратное устройство, которое защищает сеть от несанкционированного доступа, фильтруя входящий и исходящий трафик.
* Г. Протокол, который позволяет безопасно обмениваться информацией между двумя устройствами.

Ответ: В.

4. Какой тип атаки использует злоумышленник, когда пытается получить доступ к учетной записи пользователя путем перебора различных комбинаций паролей?

* А. Brute-force атака
* Б. Phishing атака
* В. Man-in-the-middle атака
* Г. Social engineering

Ответ: А.

5. Что такое криптография?

* А. Методы шифрования и дешифрования информации.
* Б. Методы анализа и прогнозирования сетевого трафика.
* В. Методы обнаружения и удаления вредоносных программ.
* Г. Методы безопасного хранения и передачи данных.

Ответ: А.

6. Какой из методов аутентификации является наиболее надежным?

* А. Пароль
* Б. Одноразовый пароль
* В. Двухфакторная аутентификация
* Г. Биометрическая аутентификация

Ответ: Г.

7. Что такое "социальная инженерия" в контексте информационной безопасности?

* А. Использование технических средств для получения доступа к информации.
* Б. Использование психологических манипуляций для получения доступа к информации.
* В. Разработка и распространение вредоносного программного обеспечения.
* Г. Анализ трафика сети для выявления подозрительной активности.

Ответ: Б.

8. Что такое "безопасный ключ" (USB-токен) и для чего он используется?

* А. Устройство для хранения паролей и других конфиденциальных данных.
* Б. Устройство для шифрования данных, передаваемых по сети.
* В. Устройство для аутентификации пользователя при доступе к информационным системам.
* Г. Устройство для обнаружения вредоносного программного обеспечения.

Ответ: В.

9. Что такое "цифровая подпись" и как она используется для обеспечения безопасности?

* А. Электронная версия рукописной подписи, которая подтверждает авторство документа.
* Б. Специальный код, который добавляется к файлу для предотвращения его копирования.
* В. Криптографический метод, который используется для проверки подлинности и целостности документа.
* Г. Специальный файл, который содержит информацию о компьютере и его владельце.

Ответ: В.

10. Какое из утверждений является наиболее верным в отношении принципа "наименьших привилегий"?

* А. Пользователям следует предоставлять доступ только к той информации, которая им необходима для выполнения своих задач.
* Б. Пользователям следует предоставлять доступ ко всей информации, которая им может потребоваться.
* В. Пользователям следует предоставлять доступ только к той информации, которую они могут понять.

* Г. Пользователям следует предоставлять доступ только к той информации, которую они могут использовать для личных целей.

Ответ: А.

Информация о разработчиках

Гурина Елена Ивановна, доцент кафедры вычислительной математики и компьютерного моделирования ММФ ТГУ.