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

Факультет инновационных технологий

УТВЕРЖДЕНО:
Декан
С. В. Шидловский

Оценочные материалы по дисциплине

Информационная безопасность

по направлению подготовки / специальности

27.03.05 Инноватика

Направленность (профиль) подготовки/ специализация:
Управление инновациями в наукоемких технологиях

Форма обучения
Очная

Квалификация
инженер-аналитик/инженер-исследователь

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
О.В. Вусович

Председатель УМК
О.В. Вусович

Томск – 2024

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

Целью освоения дисциплины является формирование следующих компетенций:

БК – 1 Способен применять общие и специализированные компьютерные программы при решении задач профессиональной деятельности

БК – 3 Способен использовать принципы и средства профессиональной коммуникации для эффективного взаимодействия

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

РОБК 1.1 Знает правила и принципы применения общих и специализированных компьютерных программ для решения задач профессиональной деятельности

РОБК 1.2 Умеет применять современные IT-технологии для сбора, анализа и представления информации; использовать в профессиональной деятельности общие и специализированные компьютерные программы

РОБК 3.1 Знает средства, функции и принципы профессиональной коммуникации

РОБК 3.2 Умеет выстраивать профессиональную коммуникацию; представлять результаты своей работы с учетом норм и правил принятых в профессиональном сообществе.

2. Оценочные материалы текущего контроля и критерии оценивания

Текущий контроль проводится в течение семестра с целью определения уровня усвоения обучающимися знаний, формирования умений и навыков, своевременного выявления преподавателем недостатков в подготовке обучающихся и принятия необходимых мер по ее корректировке, а также для совершенствования методики обучения, организации учебной работы, и фиксируется в форме контрольной точки не менее одного раза в семестр.

2.1. Тест №1

Из старой программы «Информационные технологии в управлении качеством и защита информации»:

Вопрос 1. Акустический приемник, размещаемый злоумышленником в помещении с конфиденциальной информацией, и радиоэлектронный ретранслятор, обеспечивающий достаточную дальность для съема информации злоумышленником за пределами контролируемой зоны относятся к:

1. Акусторадиоэлектронному каналу утечки информации
2. Акустооптическому каналу утечки информации
3. Акустовещественному каналу утечки информации
4. Электронному каналу утечки информации

Вопрос 2. Статья «создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации, либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами» уголовного кодекса записана под номером:

1. 272
2. 273
3. 242
4. 183

Вопрос 3. Преимущества симметричных шифров (по сравнению с асимметричными):

1. Высокая скорость (на 3 порядка быстрее асимметричных)
2. Меньшая требуемая длина ключа для сопоставимой стойкости
3. Хорошая изученность
4. Низкая скорость (на 3 порядка медленнее асимметричных)
5. Нет необходимости передавать ключи по надежному каналу связи

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

Вопросы для подготовки к зачету

1. Роль информации и её защиты в современном мире.
2. Определение защиты информации. Значение защиты информации.
3. Аспекты защиты информации.
4. Понятия безопасности информации, безопасности данных и защиты данных.
5. Понятие информационной безопасности.
6. Десять главных угроз защиты информации.
7. Понятия конфиденциальности, целостности и достоверности информации.
8. Понятия доступа к информации, санкционированный и несанкционированный доступ к информации.
9. Понятия идентификации и аутентификации.
10. Понятия угрозы информационной безопасности, уязвимости и атаки.
11. Бернская конвенция, Парижская и Берлинская конференция.
12. Римская и Брюссельская конференция. Всемирная конвенция об авторском праве.
13. Стокгольмская конференция. Особенности присоединения России к международному праву.
14. 3 статьи конституции РФ, связанные с особенностями обработки, хранения и распространения информации.
15. 4 статьи УК РФ, связанные с особенностями обработки, хранения и распространения информации.
16. Органы государственной службы РФ, играющие основную роль в создании правовых механизмов защиты информации.
17. Понятие угрозы. Виды угроз.
18. Классификация источников угроз (перечислить). Антропогенные источники угроз.
19. Классификация источников угроз (перечислить). Техногенные источники угроз.
20. Классификация источников угроз (перечислить). Стихийные источники угроз.
21. Классификация уязвимостей (перечислить). Объективные уязвимости.
22. Классификация уязвимостей (перечислить). Субъективные уязвимости.
23. Классификация уязвимостей (перечислить). Случайные уязвимости.
24. Статистика возникновения умышленных и случайных утечек.
25. Современная система удостоверяющих документов и её недостатки.
26. Бесперспективность защиты носителей и перспективы эволюции удостоверяющих документов.
27. Практика выявления поддельных документов и рекомендации, по защите документов.
28. Классификации каналов утечки информации. Структура канала утечки информации.
29. Оптический канал утечки информации.
30. Акустический канал утечки информации.
31. Радиоэлектронный канал утечки информации.
32. Материально-вещественный канал утечки информации.

33. Понятия криптографического ключа, открытого и закрытого ключа, шифрования, дешифрования и криптоанализа.
34. Понятие симметричного шифрования. Преимущества и недостатки симметричного шифрования. Виды симметричных шифров.
35. Понятие асимметричного шифрования. Преимущества и недостатки асимметричного шифрования. Виды асимметричных шифров.
36. Стандарт DES. Схема шифрования с использованием алгоритма DES. Схема работы одного цикла алгоритма DES.
37. Операционные режимы симметриного шифрования. Режим ECB.
38. Операционные режимы симметриного шифрования. Режим CBC.
39. Операционные режимы симметриного шифрования. Режим CFB.
40. Операционные режимы симметриного шифрования. Режим OFB.
41. "Тройной" DES, Rijndael, RC2.
42. Основные свойства и методы класса Symmetric Algorithm.

Критерий оценивания для промежуточной аттестации:

В основе оценивания ответов на зачёте лежат принципы объективности, справедливости и всестороннего анализа уровня знаний студентов.

«Зачтено» ставится студенту, у которого выполнены все следующие показатели:

1. Отчеты по всем 11 лабораторным работам зачтены.
2. Освещено не менее чем 70% материала контрольной работы (итоговой). Оценивается: знание фактического материала, а также культура речи, глубина знания, аргументированность ответа, связь теории и практики, умение решить задачу.
3. Получено не менее чем 70 баллов (из 100 возможных) на тест (итоговый).

«Не зачтено» ставится студенту, не имеющему всех трех показателей, описанных выше.

Информация о разработчиках

Петелин Александр Евгеньевич, доцент кафедры Информационного обеспечения инновационной деятельности Факультета инновационных технологий, кандидат физ.-мат. наук.