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

Факультет инновационных технологий

УТВЕРЖДАЮ:
Руководитель ОПОП
_____ О.В. Вусович
«30» 08 2021 г.

Оценочные материалы
текущего контроля и промежуточной аттестации по дисциплине

Информационная безопасность

по направлению подготовки

27.03.05 Инноватика

Направленность (профиль) подготовки:
Управление инновациями в наукоемких технологиях

Форма обучения
Очная

Квалификация
Бакалавр

Томск – 2021

1. Планируемые результаты освоения дисциплины

Результаты освоения дисциплины (индикатор достижения компетенции)	**Планируемые образовательные результаты (ОР) обучения по дисциплине**
ИПК-4.1 Формирование предложений по созданию (в том числе разработка соответствующего технического задания) базы данных РИД и СИ, трансфера технологий в области деятельности организации;	ОР-4.1.1 Определять требования к программному оснащению обеспечения безопасности баз данных
ИПК-4.2 Привлечение при необходимости специалистов по определенным видам профессиональной деятельности для создания базы данных РИД и СИ, трансфера технологий в области деятельности организации;	ОР-4.2.1 Определять основные требования к знаниям и умениям специалистов в политике безопасности организации
ИПК-4.3 Разработка предложений по информационному наполнению базы данных РИД и СИ, включая показатели (характеристики показателей) инновационной деятельности организации;	ОР-4.3.1 ОР-4.3.2
ИПК-4.4 Информационное наполнение базы данных РИД и СИ;	ОР-4.4.1 ОР-4.4.2
ИПК-4.5 Подготовка предложений по созданию и информационному наполнению интернет-сайта организации об объектах исключительных прав организации, его ведение и актуализация в этой части.	ОР-4.5.1 Определять требования к разработке структуры реляционных баз данных интернет-сайта с точки зрения обеспечения безопасности

2. Этапы достижения образовательных результатов в процессе освоения дисциплины

№	Разделы и(или) темы дисциплин	Образовательные результаты	Формы текущего контроля и промежуточной аттестации
1.	Тема 1. Цели и задачи дисциплины. Основные понятия и требования в области информационной безопасности	ОР-4.2.1	Тест Контрольная работа Промежуточная аттестация: Зачет
2.	Тема 2. Законодательство в области информационной безопасности	ОР-4.2.1	Тест Контрольная работа Промежуточная аттестация: Зачет
3.	Тема 3. Источники, риски и формы атак на информацию	ОР-4.2.1 ОР-4.5.1	Тест Контрольная работа Промежуточная аттестация: Зачет
4.	Тема 4. Поисковые	ОР-4.5.1	Отчет по лабораторной работе

	информационные системы		
5.	Тема 5. Резервное копирование и восстановление данных	ОР-4.1.1	Отчет по лабораторной работе
6.	Тема 6. Программные средства скрытия данных и установки пароля, очистки данных	ОР-4.1.1	Отчет по лабораторной работе
7.	Тема 7. Программы обнаружения и защиты от вредоносных программ	ОР-4.1.1	Отчет по лабораторной работе
8.	Тема 8. Криптографические методы защиты информации. Электронная подпись (ЭП). SQL-инъекции	ОР-4.5.1	Тест Контрольная работа Отчет по лабораторной работе Промежуточная аттестация: Зачет

3. Оценочные средства для проведения текущего контроля и методические материалы, определяющие процедуру их 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.

3.1. 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

Метод рекомендации по выполнению.

Критерии оценивания.

4. Оценочные средства для проведения промежуточной аттестации

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.