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

Основы информационной безопасности

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки/ специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2024

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 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

ОПК-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.

ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-1.1 Учитывает современные тенденции развития информационных технологий в своей профессиональной деятельности

ИОПК-1.2 Понимает значение информации, информационных технологий и информационной безопасности в развитии современного общества

ИОПК-1.3 Выявляет влияние информации, информационных технологий и информационной безопасности на объективные потребности личности, общества и государства

ИОПК-10.1 Осуществляет анализ тенденций развития методов и средств криптографической защиты информации

ИОПК-8.1 Осуществляет подбор, изучение и обобщение научно-технической информации, методической информации отечественного и зарубежного опыта по проблемам компьютерной безопасности

ИОПК-9.1 Учитывает современные тенденции развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных при решении задач своей профессиональной деятельности

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– тесты;

– контрольные задания.

Пример типового теста (ИОПК-1.1, ИОПК-1.2, ИОПК-1.3)

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

5. Защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации разведками и другими заинтересованными субъектами это:
а) защита информации от разглашения
б) защита информации от утечки
в) защита информации от несанкционированного доступа
г) защита информации от несанкционированного воздействия
д) защита информации от непреднамеренного воздействия

6. Защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации это:
а) защита информации от разглашения
б) защита информации от утечки
в) защита информации от несанкционированного доступа
г) защита информации от несанкционированного воздействия
д) защита информации от непреднамеренного воздействия

7. Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации это
а) информации защита информации от разглашения
б) защита информации от утечки
в) защита информации от несанкционированного доступа
г) защита информации от несанкционированного воздействия
д) защита информации от непреднамеренного воздействия

8. Защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации это:
а) информации защита информации от разглашения
б) защита информации от утечки
в) защита информации от несанкционированного доступа
г) защита информации от несанкционированного воздействия
д) защита информации от непреднамеренного воздействия

9. Защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации это:

а) информации защита информации от разглашения
б) защита информации от утечки
в) защита информации от несанкционированного доступа
г) защита информации от несанкционированного воздействия
д) защита информации от непреднамеренного воздействия

Ключи: 1 а), 2 а), 3 а) б) в), 4 б), 5 б), 6 а), 7 в), 8 г), 9 д).

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

Примеры контрольных заданий (ИОПК-10.1, ИОПК-8.1, ИОПК-9.1):

Тема “Понятийный аппарат информационной безопасности”. Используя Банк данных угроз безопасности информации ФСТЭК России (www.bdu.fstec.ru), требуется детально изучить три угрозы безопасности информации (описание угрозы, источники угрозы, объект воздействия, последствия реализации угрозы), присущих некоторому одному выбранному объекту (облачная система, грид-система, BIOS, виртуальная машина, беспроводная сеть, web-приложение, хранилище больших данных и т.п.), а также три устраненные уязвимости для некоторого выбранного ПО (СУБД MySQL, Браузер Google Chrome и т.п.). Также надо познакомиться с терминами по информационной безопасности: угроза, уязвимость, конфиденциальность, целостность, доступность (см. https://bdu.fstec.ru/terms).

Студент должен самостоятельно выполнить задание, выложить отчет в систему управления обучением Moodle, при необходимости продемонстрировать преподавателю при устной защите владение основными понятиями информационной безопасности.

Отчет включает в себя: название дисциплины и задания, ФИО и номер группы исполнителя работы, результат выполнения работы: 1) список определений терминов: угроза, уязвимость, конфиденциальность, целостность, доступность; 2) список изученных угроз и уязвимостей.

Тема “Криптографические методы защиты информации”. Требуется зашифровать свое ФИО шифром Виженера и шифром вертикальной перестановки. Студент должен самостоятельно выполнить задание, выложить отчет в систему управления обучением Moodle, при необходимости продемонстрировать преподавателю при устной защите владение материалом. Отчет включает в себя: название дисциплины и задания, ФИО и номер группы исполнителя работы, результат выполнения работы.

Тема “Средство защиты информации”. Требуется выбрать какое-либо программное средство защиты информации (СЗИ) от какого-либо производителя, изучить предназначение средства: какие задачи решаются и какие методы/подходы/алгоритмы используются для решения данных задач, архитектуру (схему работы), функциональные возможности и характеристики СЗИ. Излученный материал излагается в виде краткого реферата с указанием источников информации. После чего надо скачать и установить на своем персональном компьютере (ноутбуке) пробную версию изученного СЗИ, а также настроить СЗИ, активизируя базовые возможности продукта. Примеры СЗИ: КриптоПро

CSP – криптопровайдер, Secret Net Studio - защита конечных точек, Kaspersky Small Office Security - защита для малого бизнеса.

Студент должен самостоятельно выполнить задание, выложить отчет в систему управления обучением Moodle, при необходимости продемонстрировать преподавателю при устной защите владение материалом.

Отчет включает в себя: название дисциплины и задания, ФИО и номер группы исполнителя работы, результат выполнения работы в виде реферата и скриншотов (снимков экрана) с настройками СЗИ.

Выполнение контрольных заданий оценивается по двоичной системе (зачет/незачет): студент получает зачет, когда он показал, что в целом удовлетворительно разбирается в задаче, хорошо знает материал, возможно имеются негрубые ошибки; студент получает зачет, когда он слабо разбирается в задаче, плохо знает материал, не отвечает, либо отвечает, но с ошибками на вопросы преподавателя.

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

Зачет проводится на основе проверки выполнения контрольных заданий и/или по результатам собеседования с использованием перечня вопросов по курсу. Схема вопросов зачета соответствует компетентностной структуре дисциплины. Продолжительность зачета 1 час.

Примерный перечень вопросов к зачету (ИОПК-1.1, ИОПК-1.2, ИОПК-1.3, ИОПК-10.1, ИОПК-8.1, ИОПК-9.1):

1. Уровни представления информации.
2. Свойства защищаемой информации.
3. Виды тайн (государственная, служебная, профессиональная,…).
4. Термины, относящиеся к видам защиты информации.
5. Термины, относящиеся к способам защиты информации.
6. Термины, относящиеся к замыслу защиты информации.
7. Термины, относящиеся к объекту защиты информации.
8. Термины, относящиеся к угрозам безопасности информации.
9. Термины, относящиеся к технике защиты информации.
10. Национальная безопасность РФ.
11. Доктрина информационной безопасности РФ.
12. Законодательная основа обеспечения информационной безопасности.
13. Нормативная основа обеспечения информационной безопасности.
14. Безопасность критической информационной инфраструктуры РФ.
15. Государственная система обеспечения информационной безопасности.
16. Несанкционированные операции с информацией.
17. Источники и классификация угроз.
18. Перечень типовых непреднамеренных искусственных угроз.
19. Перечень типовых преднамеренных искусственных угроз.
20. Классификация способов несанкционированного доступа.
21. Типовые атаки на коммуникационные протоколы.
22. Законодательные меры противодействия угрозам безопасности.
23. Организационные меры противодействия угрозам безопасности.
24. Физические и технические меры противодействия угрозам безопасности.

25. Аутентификация. Невозможность отказа от авторства.
26. Имитозащита. Цифровая подпись.
27. Симметричный / асимметричный шифр.
28. Криптографическая стойкость шифра.
29. Метод криптографического анализа.
30. Криптографический протокол.
31. Криптографическая хеш-функция.
32. Классификация криптопротоколов.
33. Свойства цифровой подписи.
34. Криптографические протоколы аутентификации сообщений.
35. Криптографические протоколы идентификации.
36. Объект, субъект, доступ к информации, правила разграничения доступа.
37. Идентификация, аутентификация, авторизация.
38. Протоколирование и аудит (активный аудит).
39. Статистический метод обнаружения атак.
40. Сигнатурный метод обнаружения атак.
41. Дискреционное управление доступом.
42. Мандатное управление доступом.
43. Ролевое управление доступом.
44. Защита информации при хранении и передаче.
45. Защита от вредоносных программ.
46. Виды компьютерных вирусов и вредоносных программ.
47. Защита межсетевого взаимодействия.
48. Предотвращение утечек информации.
49. Аудит безопасности.
50. Угрозы корпоративной сети. Защита периметра сети.
51. Основные механизмы защиты корпоративной сети.
52. Средства защиты информации: межсетевые экраны.
53. Средства защиты информации: виртуальные частные сети.
54. Средства защиты информации: системы анализа защищенности.
55. Средства защиты информации: системы обнаружения атак.
56. Системы предотвращения утечки конфиденциальной информации.
57. Политика информационной безопасности организации.

Результаты зачета определяются оценками «зачтено», «не зачтено»:

оценка «зачтено» ставится, если студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал требуемые умения и навыки при выполнении большинства (>80%) тестовых/контрольных заданий.

оценка «не зачтено» ставится, если студент имеет существенные пробелы по отдельным теоретическим разделам дисциплины и/или не показал требуемые умения и навыки при выполнении тестовых/контрольных заданий (выполнено менее 80% заданий).

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

Тест (ИОПК-1.1, ИОПК-1.2, ИОПК-1.3)

1. Защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации разведками и другими заинтересованными субъектами это:

a) защита информации от разглашения
b) защита информации от утечки
c) защита информации от несанкционированного доступа
d) защита информации от несанкционированного воздействия
e) защита информации от непреднамеренного воздействия

2. Защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации это:

a) защита информации от разглашения
b) защита информации от утечки
c) защита информации от несанкционированного доступа
d) защита информации от несанкционированного воздействия
e) защита информации от непреднамеренного воздействия

3. Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации это

a) защита информации от разглашения
b) защита информации от утечки
c) защита информации от несанкционированного доступа
d) защита информации от несанкционированного воздействия
e) защита информации от непреднамеренного воздействия

4. Защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации это:

a) защита информации от разглашения
b) защита информации от утечки
c) защита информации от несанкционированного доступа
d) защита информации от несанкционированного воздействия
e) защита информации от непреднамеренного воздействия

5. Защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации это:

a) защита информации от разглашения
b) защита информации от утечки

c) защита информации от несанкционированного доступа
d) защита информации от несанкционированного воздействия
e) защита информации от непреднамеренного воздействия

Ключи: 1 b), 2 a), 3 c), 4 d), 5 e).

Примерный перечень контрольных вопросов для проверки остаточных знаний (при оценивании необходимо продемонстрировать достижение **всех** запланированных индикаторов достижения компетенций):

1. Несанкционированные операции с информацией.
2. Источники и классификация угроз безопасности информации.
3. Типовые непреднамеренные искусственные угрозы.
4. Типовые преднамеренные искусственные угрозы.
5. Классификация способов несанкционированного доступа.
6. Типовые атаки на коммуникационные протоколы.
7. Законодательные меры противодействия угрозам безопасности.
8. Организационные меры противодействия угрозам безопасности.
9. Физические и технические меры противодействия угрозам безопасности.
10. Аутентификация. Имитозащита. Цифровая подпись.
11. Симметричные шифры. Асимметричные шифры.
12. Криптографические протоколы.
13. Криптографические хеш-функции.
14. Идентификация, аутентификация, авторизация.
15. Протоколирование и аудит (активный аудит).
16. Дискреционное управление доступом.
17. Мандатное управление доступом.
18. Ролевое управление доступом.
19. Виды компьютерных вирусов и вредоносных программ.
20. Защита межсетевого взаимодействия.
21. Основные механизмы защиты корпоративной сети.
22. Основные средства защиты корпоративной сети

Информация о разработчиках

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