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

Механико-математический факультет

УТВЕРЖДЕНО:
Декан ММФ ТГУ
Л.В.Гензе

Оценочные материалы по дисциплине

**Основы информационной безопасности**
по направлению подготовки

**01.03.01 Математика**
**02.03.01 Математика и компьютерные науки**
**01.03.03 Механика и математическое моделирование**

Направленность (профиль) подготовки
**Основы научно-исследовательской деятельности в области математики**
**Основы научно-исследовательской деятельности в области математики и компьютерных наук**
**Основы научно-исследовательской деятельности в области механики и математического моделирования**

Форма обучения
**Очная**

Квалификация
**Бакалавр**

Год приема
**2023**

СОГЛАСОВАНО:
Руководитель ОП
Л.В.Гензе

Председатель УМК
Е.А.Тарасов

Томск – 2023

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

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-6 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности, с учетом основных требований информационной безопасности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК 6.1 Показывает владение базовыми знаниями по защите информации на рабочем месте и при входе в локальные и глобальные сети

ИОПК 6.2 Применяет знания принципов работы современных информационных технологий при решении задач профессиональной деятельности, с учетом требований информационной безопасности

**2. Оценочные материалы текущего контроля и критерии оценивания**

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения тестов по лекционному материалу, и фиксируется в форме контрольной точки не менее одного раза в семестр.

Элементы текущего контроля:

– тесты.

**Тест** (ИОПК 6.1, ИОПК 6.2)

1. Какие из нижеперечисленных уровней информационной безопасности необходимы, чтобы обеспечить комплексный подход и добиться успеха в деле обеспечения информационной безопасности:
   а) законодательный;
   б) программно-технический;
   в) процедурный;
   г) специально создаваемый;
   д) административный.

2. Это метод шифрования данных, в котором исходный текст разделяется на блоки фиксированного размера и шифруется с использованием ключа. Этот тип шифрования является одним из основных элементов современной криптографии и широко используется для обеспечения безопасности данных во многих областях, таких как интернет-банкинг, электронная коммерция и коммуникации:
   а) блочный шифр;
   б) поточный шифр;
   в) стенография;
   г) сжатие.

3. Это вид симметричного шифрования, при котором отдельные символы открытого текста (обычно биты или байты) преобразуются в зашифрованный текст путем объединения с ключевой последовательностью:
   а) блочный шифр;
   б) поточный шифр;
   в) стенография;
   г) сжатие.

**4.** Термины «Интернет» и «Всемирная сеть» являются взаимозаменяемыми:
а) верно;
б) неверно.

5. Это форма межгосударственного соперничества, реализуемая посредством оказания информационного воздействия на системы управления других государств и их вооруженных сил, а также на политическое и военное руководство и общество в целом, информационную инфраструктуру и средства массовой информации этих государств для достижения выгодных для себя целей при одновременной защите от аналогичных действий своего информационного пространства:

   а) информационная война;
   б) информационное противоборство;
   в) информационная преступность;
   г) информационное оружие.

6. Назовите основные задачи системы информационной безопасности. Выберите правильные варианты:

   а) эффективное пресечение посягательств на ресурсы и угроз персоналу на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;
   б) своевременное выявление и устранение угроз безопасности и ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба;
   в) создание механизма и условий оперативного реагирования на угрозы безопасности в функционировании предприятия. А также ослабление негативного влияния последствий нарушения безопасности на достижение целей организации.

7. Информация может передаваться различными способами, включая поля, вещества и другие среды. Какой из основных способов передачи информации отсутствует в списке (напишите):
   - физические волны и поля;
   - вещества;
   - цифровые системы;
   - ...

8. Логическая бомба (как тип вредоносного ПО) - это программа, которая способна копироваться и распространяться между компьютерами, заражая другие файлы и системы. Может передаваться по электронной почте, съемным носителям и сетям:
   а) верно;
   б) неверно.

9. Это свойство (характеристика) информации, указывающее на необходимость ограничения круга субъектов, имеющих доступ к данной информации:
   а) конфиденциальность;
   б) целостность;
   в) доступность;
   г) функциональность.

10. Согласно классификации информационного оружия, выберите те из вариантов,

в которых главным объектом воздействия ИО являются люди. Выберите правильные варианты:

а) средства специального программно-технического воздействия;
б) системы активного радиоэлектронного противодействия;
в) психотронные генераторы;
г) СМИ;
д) средства радиоэлектронной борьбы;
е) разведка.

11. Комплекс технических и других средств, методов технологий, предназначенных для:

- установления контроля над информационными ресурсами потенциального противника;

- вмешательство в работу его систем управления и информационных сетей, систем связи и т.п. в целях нарушения их работоспособности, вплоть до полного выведения из строя, изъятия, искажения содержащихся в них данных или направленного введения специальной информации;

- распространение выгодной информации и дезинформации в системе формирования общественного мнения и принятия решений;

- воздействие на сознание и психику политического и военного руководства, личного состава вооруженных сил, спецслужб и населения противостоящего государства, используемых для достижения превосходства над противником или ослабления проводимых им информационных воздействий:

а) информационная война;
б) информационное противоборство;
в) информационная преступность;
г) информационное оружие.

12. Проведение информационных воздействий на информационное пространство или любой его элемент в противоправных целях. Частный случай - информационный терроризм, то есть деятельность, проводимая в политических целях:

а) информационная война;
б) информационное противоборство;
в) информационная преступность;
г) информационное оружие.

13. На каких из нижеследующих уровнях военных действий проводятся информационные операции. Выделите необходимые уровни:

а) на тактическом уровне;
б) на программно-техническом уровне;
в) на стратегическом уровне;
г) на оперативном уровне.

14. Напишите своими словами, что вы понимаете под каналами утечки информации ограниченного доступа.

15. Напишите своими словами, на чем основаны криптографические методы защиты информации? И в чем смысл данных методов?

**Ключи**:
1 а), б), в), д)
2 а)
3 б)
4 б)
5 б)
6 а), б), в)
7 биологический
8 б)
9 а)
10 в), г)
11 г)
12 в)
13 а), в), г)
14 Каналы утечки информации ограниченного доступа – это пути, по которым конфиденциальная информация может быть раскрыта, передана или скомпрометирована без разрешения. В контексте информационной безопасности, такие каналы создают серьезные угрозы для сохранения целостности, доступности и конфиденциальности информации.
15 Данные методы основаны на преобразовании информации перед ее хранением и передачей на основе секретного параметра (ключа) таким образом, чтобы привести информацию к ее открытому виду или смысловому содержанию мог только обладатель ключа. Смысл данных методов: заключается именно в том, чтобы только обладатель ключа смог в дальнейшем манипулировать информацией.

**Критерии оценивания**: тест считается пройденным, если обучающийся ответил правильно не менее чем на 10 вопросов.

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

Самостоятельная работа студентов по курсу «Основы информационной безопасности» завершается подготовкой реферата по одной из выбранных тем, проверяющих ИОПК 6.1 и ИОПК 6.2. Тема согласовывается с преподавателем.

**Типовые темы для самостоятельной работы по курсу (**ИОПК 6.1 и ИОПК 6.2**):**

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;

**Теоретический опрос студентов на зачетном занятии состоит из двух частей**:

Первая часть содержит 2 вопроса, проверяющих ИОПК 6.1. Ответы на вопросы первой части могут быть краткими и предполагают владение базовыми знаниями по защите информации.

Вторая часть содержит один вопрос, проверяющий ИОПК 6.2. Ответ на вопрос второй части дается в развернутой форме.

**Типовые вопросы для проведения промежуточной аттестации в форме зачета:**

1. Понятие информационной безопасности (ИОПК 6.1);
2. Основные составляющие информационной безопасности (ИОПК 6.1);
3. Собственник, владелец информации. Правила отнесения информации к защищаемой (ИОПК 6.1);
4. Что такое защита информации (ИОПК 6.1, ИОПК 6.2)?
5. Что такое конфиденциальность (ИОПК 6.1)?
6. Основные угрозы информационной безопасности. Классификация угроз (ИОПК 6.1);
7. Законодательный уровень информационной безопасности и почему он важен (ИОПК 6.1, ИОПК 6.2)?
8. Законодательные акты в области информационной безопасности (ИОПК 6.1);
9. Какие сведения составляют государственную тайну (ИОПК 6.1)?
10. Государственная тайна ее существенные признаки (ИОПК 6.1);
11. Порядок засекречивания информации, составляющей государственную тайну (ИОПК 6.1, ИОПК 6.2);
12. Основания для рассекречивания сведений, составляющих государственную тайну (ИОПК 6.1, ИОПК 6.2);
13. Национальные интересы РФ в информационной сфере и их обеспечение (ИОПК 6.2);
14. Источники угроз информационной безопасности РФ (ИОПК 6.1, ИОПК 6.2);
15. Сущность и особенности информационной войны (ИОПК 6.1);
16. Методы и приемы современных информационных войн (ИОПК 6.1, ИОПК 6.2);
17. Информационная война. Традиционные методы и новые тенденции (ИОПК 6.1);
18. Что такое персональные данные и почему они важны (ИОПК 6.1, ИОПК 6.2)?
19. Способы защиты персональных данных (ИОПК 6.2);
20. Принципы защиты информации при передаче данных (ИОПК 6.1, ИОПК 6.2);

21. Защита информации на жестком диске (ИОПК 6.2);
22. Защита информации в локальных вычислительных сетях (ИОПК 6.1, ИОПК 6.2);
23. Проблема защиты информации в корпоративных сетях и почему она актуальна (ИОПК 6.2)?
24. Модель взаимодействия открытых систем OSI (ИОПК 6.1, ИОПК 6.2);
25. Модель и стек протоколов TCP/IP (ИОПК 6.1, ИОПК 6.2);
26. Понятие вредоносной программы (ИОПК 6.1);
27. Классификация вредоносных программ (ИОПК 6.1);
28. Основные способы распространения вредоносных программ (ИОПК 6.1, ИОПК 6.2);
29. Основные организационные мероприятия, производимые для защиты от компьютерных вирусов (ИОПК 6.1, ИОПК 6.2);
30. Признаки заражения ПК вирусом. Выбор антивирусной программы (ИОПК 6.1, ИОПК 6.2).

**Критерии оценивания:**

При проведении аттестации в форме зачета в конце семестра обучающемуся, успешно прошедшему тестирование по лекционному материалу и сдавшему реферат, дается три вопроса, в которых требуется по заданной теме дать определение ряда понятий, сформулировать ответы и проиллюстрировать их примерами. “Зачет” ставится в том случае, если обучающийся ответил на два вопроса.

Вне зависимости от результатов текущей успеваемости (тест не пройден/не набран проходной балл) студент имеет право проходить промежуточную аттестацию. В этом случае студенту, сдавшему реферат дается 5 вопросов. “Зачет” ставится в том случае, если обучающийся ответил на четыре вопроса.

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

Элементы контроля остаточных знаний:
– теоретические вопросы.

Теоретические вопросы:

1. Дайте понятие информационной безопасности в узком смысле (ИОПК 6.1);

Ответ должен содержать информацию о надёжности работы компьютера, сохранности ценных данных и защиту информации от внесения в нее изменений неуполномоченными лицами, а также о тайне переписки в электронной среде.

2. Что понимается под угрозой безопасности информации (ИОПК 6.2)?
3. Опишите такое свойство информации, как конфиденциальность (ИОПК 6.1);

Ответ дать с точки зрения системы основных составляющих информационной безопасности.

4. Опишите такие свойства информации, как целостность и доступность (ИОПК 6.1);
5. Перечислите стратегические задачи информационной войны (ИОПК 6.1);
6. В зависимости от масштабов информационные войны делятся на персональные, корпоративные и глобальные. Дайте краткое определение каждого из перечисленных понятий (ИОПК 6.1);
7. К основным способам передачи информации относятся физические волны и поля, вещества, биологические сигналы, цифровые системы. Поясните, как именно информация может передаваться через каждый из них (ИОПК 6.2);

8. Что именно понимается под каналом утечки информации (ИОПК 6.1)?

9. Что является носителем информации в инфо-телекоммуникационных каналах (ИОПК 6.1, ИОПК 6.2)?

10. На чем основаны криптографические методы защиты информации. Поясните смысл данных методов и для обеспечения каких составляющих информационной безопасности они предназначены (ИОПК 6.2)?

11. Какие два основных типа шифрования существуют (ИОПК 6.1)?

12. В чем сложность самостоятельного изучения компьютерных сетей (ИОПК 6.1, ИОПК 6.2)?

13. Осуществите классификацию сетей по технологии передачи данных (ИОПК 6.1);

14. Что вы знаете о такой эталонной модели компьютерных сетей, как модель взаимодействия открытых систем ISO OSI (ИОПК 6.2)?

15. Сколько уровней включает в себя эталонная модель компьютерных сетей TCP/IP (ИОПК 6.2)?

**Информация о разработчиках**

Гурина Елена Ивановна, кандидат физико-математических наук, доцент.