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

Механико-математический факультет

УТВЕРЖДАЮ:
Декан
_____Л. В.Гензе
«20» 06 2022 г.

Рабочая программа дисциплины

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
2022

Код дисциплины в учебном плане: Б1.О.2.10

СОГЛАСОВАНО:
Руководитель ОП
_____Л. В.Гензе

Председатель УМК
_____Е.А. Тарасов

Томск – 2022

1. Цель и планируемые результаты освоения дисциплины

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. Задачи освоения дисциплины

– Освоить основы организационной и правовой защиты информации, ее современные проблемы и терминологию; изучить основные документы, регламентирующие организационную безопасность на объекте;

– Научиться оценивать состояние организационной защиты информации на объекте;

– Овладеть навыками выявления угроз информационной безопасности объекта.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к Блоку 1 «Дисциплина (модули)».
Дисциплина относится к обязательной части образовательной программы.

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Второй семестр, зачет

5. Входные требования для освоения дисциплины

Пререквизиты – отсутсвуют.
Параллельно осваиваемые дисциплины – программирование, компьютерные науки.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 2 з.е., 72 часов, из которых:
-лекции: 16 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. *Понятие информационной безопасности.*
Основные составляющие. Важность проблемы

Краткое содержание темы:
Понятие информационной безопасности в узком смысле слова подразумевает:
- надежность работы компьютера;
- сохранность ценных данных;
- защиту информации от внесения в нее изменений неуполномоченными лицами;
- сохранение тайны переписки в электронной среде.

В данной теме понятие информационной безопасности рассматривается, как одно из базовых в информационном праве. Рассматриваются подробно основные задачи системы ИБ, а также такие понятия, как информация, информационное общество и информационные ресурсы. Детально обсуждается система основных составляющих информационной безопасности и поясняются понятия доступности, целостности и конфиденциальности.

Тема 2. *Законодательный уровень информационной безопасности*.

Краткое содержание темы:

В наиболее общем виде информационная безопасность может быть определена как невозможность нанесения вреда свойствам объекта безопасности, обуславливаемым информацией и информационной инфраструктурой.

Так в Российской Федерации, в соответствии с современной стратегией национальной безопасности, к основным объектам безопасности относятся: - личность (её конституционные права), - общество (его свободы, достойные качество и уровень жизни граждан), - государство (его суверенитет, территориальная целостность и устойчивое развитие Российской Федерации, оборона и безопасность).

В данном разделе изучаются Государственные органы РФ, обеспечивающие информационную безопасность, а также службы, организующие защиту информации на уровне предприятий.

Рассматривается каждый из уровней информационной безопасности:

- законодательный;
- административный;
- процедурный;
- программно-технический.

Тема 3. Информационная война, методы и средства её ведения.

Краткое содержание темы:

В данной теме рассматриваются понятие информационной войны, проблемы информационной войны. Информационное оружие и его классификация. Цели информационной войны, её составные части и средства её ведения. Информационная война как угроза национальной безопасности. Объекты воздействия в информационной войне.

Подробно рассматриваются уровни ведения информационной войны:

- информационные операции;
- психологические операции;
- оперативная маскировка;
- радиоэлектронная борьба;
- воздействие на сети.

Тема 4. Информационная безопасность вычислительных сетей. ИБ при использовании Internet.

Краткое содержание темы:

В данной теме рассматриваются каналы утечки информации ограниченного доступа и методы несанкционированного доступа к конфиденциальной информации.

Изучаются следующие группы каналов утечки информации:

– организационные каналы утечки информации (О-КУИ);
– технические каналы утечки информации (Т-КУИ);
– инфо-телекоммуникационные каналы утечки информации (ИТК-КУИ);
– системно-программные каналы утечки информации (СП-КУИ);
– комбинированные каналы утечки информации (К-КУИ).

Тема 5. ИБ компьютеров и компьютерных сетей.

Краткое содержание темы:

В данном разделе рассматривается модель нарушителя безопасности автоматизированной системы. Изучаются принципы работы сетей (рассматриваются ключевые технологии и протоколы, роли каждого протокола и технологии, а также схемы взаимодействия между ними). Рассматривается классификация сетей по типу коммутации, по технологиям передачи, по протяженности. Изучается сетевое взаимодействие, рассматриваются общие принципы топологии компьютерных сетей.

Тема 6. Безопасность операционных систем.

Краткое содержание темы:

Под безопасностью любой операционной системы можно понимать ее способность обладать свойствами конфиденциальности, доступности и целостности хранимой информации. Под угрозой в данном случае следует понимать любое потенциальное действие, которое направлено на нарушение одного из трех основных составляющих информационной безопасности или всех одновременно. В данном разделе рассматриваются два основных подхода к созданию защищенных ОС – фрагментарный и комплексный, а также основные административные меры защиты.

Тема 7. Компьютерные вирусы и защита от них.

Краткое содержание темы:

В данной теме рассматриваются методы несанкционированного доступа с использованием системно-программного канала:

– «маскировка под зарегистрированного пользователя»;

– использование дефектов программного обеспечения («люков» и др.)

– использование программных закладок;

– применение программных вирусов.

Рассматривается классификация вредоносных программ. Изучаются признаки, лежащие в основе классификации компьютерных вирусов.

Тема 8. Заключение. В последней лекции подводится итог курса. Далее предполагается самостоятельная работа студента по курсу. Написание реферата по выбранной и согласованной с преподавателем теме, а также подготовка доклада по теме

9. Текущий контроль по дисциплине

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.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Самостоятельная работа студентов по курсу «Основы информационной безопасности» завершается подготовкой доклада и написанием реферата по одной из выбранных тем для самостоятельной работы. Тема согласовывается с преподавателем.

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. “Зачет” ставится в том случае, если обучающийся ответил на два вопроса.

Типовые темы для самостоятельной работы по курсу:

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.

Типовые вопросы для проведения промежуточной аттестации в форме зачета:

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.

Результаты зачета определяются по двухбалльной системе «зачтено», «не зачтено».

Проставляется «зачтено» если:
- Студент выполнил индивидуальное задание, подготовил реферат по теме и успешно защитил доклад;
- Ответил на два вопроса.

Проставляется «не зачтено» если:
- Студент ответил правильно менее чем на два вопроса и не смог выполнить индивидуальное задание (не подготовил реферат и не защитил доклад).

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - https://moodle.tsu.ru/course/view.php?id=8366

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине.

в) Для успешного освоения материала студентам необходимо посещать занятия, а во время самостоятельной работы пользоваться источниками, информационными системами и базами данных, которые представлены в списке литературы. Самостоятельная работа студентов состоит в проработке лекционного материала и самостоятельного изучения дополнительных вопросов для получения более глубоких теоретических сведений по тематике защищаемого реферата. Студенты должны внимательно относиться к подготовке доклада и написанию реферата по выбранной теме, уверенно отвечать на вопросы по тематике работы.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Зайцев А.П. Технические средства и методы защиты информации. - М: Горячая линия-Телеком, 2012 г., 615 с.
– Ищейнов В.Я. Защита конфиденциальной информации. -М: Форум, 2013 г., 256 с.

– Царегородцев А.В. Технические средства защиты информации. Учебник. –М.: Изд. ВГНА Минфина России, 2009.
– Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. -М: ФОРУМ, 2013 г., 592 с.
– Галатенко В.А. Основы информационной безопасности. - М.: ИНТУИТ.РУ “Интернет-Университет Информационных Технологий”, 2003. - 280 с.
– Мещеряков Р.В., Шелупанов А.А., Белов Е.Б., Лось В.П. Основы информационной безопасности. - Томск.: ТУСУР, 2002. – 350 с.

б) дополнительная литература:

– Торокин А.А. Основы инженерно-технической защиты информации. - М.: «Ось-89», 1998.
– Хорев А.А. Защита информации от утечки по техническим каналам утечки информации. Часть 1. Технические каналы утечки информации. - М.: Гостехкомиссия России, 1998.
– Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.
– Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. – М.: Мир, 1999. – 351 с.

в) ресурсы сети Интернет:

– https://openedu.ru/ – сайт обучающих курсов ведущих вузов России;
– https://stepik.org/ – сайт онлайн-курсов от ведущих вузов и компаний страны;
– http://elibrary.ru/ - Научная электронная библиотека.

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:
– Операционная система: Microsoft Windows 10;
– Microsoft Office Standart 2013.

б) информационные справочные системы:
– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system
– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index
– ЭБС Лань – http://e.lanbook.com/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

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