

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

Факультет инновационных технологий

УТВЕРЖДЕНО:

Декан

С. В. Шидловский

Рабочая программа дисциплины

Информационная безопасность

по направлению подготовки / специальности

09.03.02 Информационные системы и технологии

Направленность (профиль) подготовки/ специализация:

Программное и аппаратное обеспечение беспилотных авиационных систем

Форма обучения

Очная

Квалификация

Инженер - программист

Инженер - разработчик

Год приема

2025

СОГЛАСОВАНО:

Руководитель ОП

С. В. Шидловский

Председатель УМК

О.В. Вусович

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-2 Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности.

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

РООПК-2.1 Знает принципы работы современных информационных технологий и программных средств (в том числе отечественного производства) при решении задач профессиональной деятельности

РООПК-2.2 Умеет осуществлять выбор информационных технологий и программных средств в зависимости от поставленной задачи

РООПК-3.1 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности

РООПК-3.2 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

2. Задачи освоения дисциплины

– Освоить аппарат обеспечения безопасности хранения данных на персональном компьютере в файловой системе и базах данных и применять его для информационного наполнения интернет-сайта организации, в т.ч. базы данных.

– Научиться применять аппарат скрещения и восстановления данных, установки пароля и шифрования данных.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к Блоку 1 «Дисциплины (модули)».

Дисциплина относится к обязательной части образовательной программы.

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

Девятый семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Теория систем управления.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 2 з.е., 72 часов, из которых:

-лекции: 14 ч.

-практические занятия: 18 ч.

Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Цели и задачи дисциплины. Основные понятия и требования в области информационной безопасности.

Роль информации в современном мире. Значение и аспекты защиты информации. Основные понятия и определения: безопасность информации, безопасность данных, защита данных, информационная безопасность, конфиденциальность информации, санкционированные и несанкционированный доступ к информации, идентификация и аутентификация, угроза информационной безопасности, уязвимость, атака. Главные типы угроз защиты информации.

Тема 2. Законодательство в области информационной безопасности

История развития международного права в области информационной безопасности. Статьи конституции РФ и уголовного кодекса РФ в области информационной безопасности. Органы государственной власти, играющие основную роль в создании правовых механизмов защиты информации

Тема 3. Источники, риски и формы атак на информацию

Классификация угроз безопасности информации. Технические каналы утечки информации. Система управления рисками.

Тема 4. Поисковые информационные системы

Составление запросов в популярных поисковых информационных системах google и yandex. Поиск документов в сети Интернет.

Тема 5. Резервное копирование и восстановление данных

Принцип хранения данных на жестком диске. Теоретические основы восстановления данных. Восстановление файлов, удаленных с внешнего носителя информации.

Тема 6. Программные средства скрытия данных и установки пароля, очистки данных

Проприетарные программное обеспечение скрытия и установки пароля, очистки данных.

Тема 7. Программы обнаружения и защиты от вредоносных программ

Антивирусы и фаерволы. Описание и сравнение.

Тема 8. Криптографические методы защиты информации. Электронная подпись (ЭП). SQL-инъекции

Симметричные и асимметричные алгоритмы шифрования данных. Электронная подпись (ЭП). Электронные сертификаты. Реализация криптографических алгоритмов в среде VisualStudio на языке программирования C#. SQL-инъекции.

Практические задания

№	Тема практического задания
1.	Формирование политики безопасности Выявление и описание источников и форм атак на информацию, оценка рисков
2.	Поиск документов в сети Интернет Использование языка поисковых запросов в google и yandex для поиска необходимых

	документов
3.	Восстановление данных Восстановление файлов, удаленных с внешнего носителя информации
4.	Программные средства информационной безопасности Скрытие и установки пароля на файлы и папки, очистки данных
5.	Настройка безопасности в операционной системе Windows Настройка браузера, ограничение возможности сетевого доступа, профилактика заражения реестра, управление правами пользователей, в т.ч. настройка паролей пользователей
6.	Антивирусные программные средства обеспечения информационной безопасности Проверка файлов и url с использованием онлайн антивирусов. Использование песочницы. Поиск вредоносных программ на компьютере.
7.	Фаервол Настройка встроенного фаервола Windows и проприетарного фаервола
8.	Простейшие алгоритмы шифрования Шифр Цезаря, шифр Виженера, шифр Плейфера
9.	Симметричные алгоритмы шифрования информации Реализация программы шифрования с использованием симметричных алгоритмов шифрования
10.	Асимметричные алгоритмы шифрования информации Реализация программы шифрования с использованием асимметричных алгоритмов шифрования
11.	Электронная подпись Реализация программы создания и проверки цифровой подписи

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем проведения контрольных работ, тестов по лекционному материалу, отчетов по выполнению практических заданий и фиксируется в форме контрольной точки не менее одного раза в семестр.

Оценочные материалы текущего контроля размещены на сайте ТГУ в разделе «Информация об образовательной программе» - <https://www.tsu.ru/sveden/education/eduop/>.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Зачет в девятом семестре проводится в виде итогового теста в электронном учебном курсе по дисциплине в среде электронного обучения «iDO».

Оценочные материалы для проведения промежуточной аттестации размещены на сайте ТГУ в разделе «Информация об образовательной программе» - <https://www.tsu.ru/sveden/education/eduop/>.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в среде электронного обучения «iDO» – <https://lms.tsu.ru/course/index.php?categoryid=3011>

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

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

1. Бабаш А.В. Актуальные вопросы защиты информации: монография / А.В. Бабаш, Е.К. Баранова – М.: ИНФРА-М, 2020. – 110 с.

2. Бузов Г.А. Выявление специальных технических средств несанкционированного получения информации / Г.А. Бузов – М.: Горячая линия - Телеком 2019. – 203 с.

3. Козьминых С.И. Обеспечение комплексной защиты объектов информатизации : [учебное пособие для студентов вузов, обучающихся по направлению "Информационная безопасность", квалификация (степень) "магистр"] / С.И. Козьминых ; Финансовый ун-т при Правит. Рос. Фед. – М.: ЮНИТИ-ДАНА 2020. – 543 с.

4. Швечкова О.Г. Базовые криптографические алгоритмы защиты информации : учебное пособие: [для студентов высших учебных заведений, обучающихся по направлениям подготовки 2.09.03.04 "Программная инженерия" и 2.09.03.03 "Прикладная информатика"] / О.Г. Швечкова, А.Н. Пылькин, Д.В. Марчев – М.: Курс 2020. – 167 с.

б) дополнительная литература:

1. Ворона В.А. Теоретические основы обеспечения безопасности объектов информатизации: учебное пособие для вузов по направлению "Информационная безопасность" / В.А. Ворона, В.А. Тихонов, Л.В. Митрякова. – М.: Горячая Линия-Телеком, 2016. – 303 с.

2. Грушо А.А. Теоретические основы компьютерной безопасности: учебное пособие для студентов вузов, обучающихся по специальностям группы 090100 "Информационная безопасность"/ А.А. Грушо, Э.А. Применко, Е.Е. Тимонина. – М.: Академия, 2009. – 267 с.

3. Девянин П. Модели безопасности компьютерных систем. Управление доступом и информационными потоками / П. Девянин. – Изд-во: Горячая Линия - Телеком, 2013. – 338 с.

4. Зайцев А.П. Технические средства и методы защиты информации: учебник для студентов вузов по группе специальностей - "Информационная безопасность" / А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов. – М. : Горячая Линия-Телеком, 2016. – 442 с.

5. Петелин А.Е. Информационная безопасность: учебно-методический комплекс [для студентов вузов по направлению 23.07.00 "Прикладная информатика"]. Том. гос. ун-т. – Томск: Томский государственный университет, 2016. URL: <http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000534758>

6. Проскурин В.Г. Защита в операционных системах: учебное пособие [для студентов (слушателей) вузов, обучающихся по специальностям 10.05.01 – "Компьютерная безопасность", 10.05.03 – "Информационная безопасность автоматизированных систем" и 10.05.04 – "Информационно-аналитические системы безопасности", по направлению подготовки 10.03.01 – "Информационная безопасность", уровень бакалавр] / В.Г. Проскурин. – М. : Горячая Линия-Телеком, 2016. – 192 с.

7. Таненбаум Э.С. Современные операционные системы / Э.С. Таненбаум. – СПб.: Питер, 2010. – 1115 с.

8. Хаулет Т. Защитные средства с открытыми исходными текстами / Т. Хаулет. – М: Интернет-Университет информационных технологий [и др.], 2010. – 607 с.

9. Шелухин О.И. Стеганография. Алгоритмы и программная реализация : [учебное пособие для студентов вузов по направлению подготовки 11.03.02. 11.04.02 - "Инфокоммуникационные технологии и системы связи" квалификации (степени) "бакалавр" и "магистр"] / О.И. Шелухин, С.Д. Канаев; под ред. О.И. Шелухина – М.: Горячая линия - Телеком 2018. – 592 с.

10. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер – Триумф, 2002. – 816 с.

в) ресурсы сети Интернет:

1. Информационная безопасность. Защита информации [Электронный ресурс] – Электрон. дан. – URL: <http://all-ib.ru/>.

2. Comparison of antivirus software [Электронный ресурс] – Электрон. дан. – URL: http://en.wikipedia.org/wiki/Comparison_of_antivirus_software.

3. Угрозы информационной безопасности в АС [Электронный ресурс] – Электрон. дан. – URL: <http://asher.ru/security/book/its/05>

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:
– Microsoft Visual Studio Community (свободно распространяемая версия Visual Studio для обучения программированию);
– публично доступные облачные технологии (Яндекс диск).

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/>
– ЭБС Консультант студента – <http://www.studentlibrary.ru/>
– Образовательная платформа Юрайт – <https://urait.ru/>
– ЭБС ZNANIUM.com – <https://znanium.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.

Для проведения лабораторных работ необходимо лицензионное программное обеспечение: Microsoft Office стандартный 2010, браузер последней версии.

15. Информация о разработчиках

Самохина Светлана Ивановна, кандидат физ.-мат. наук, доцент, доцент кафедры интеллектуальных технических систем факультета инновационных технологий НИ ТГУ.