

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

САЕ Институт «Умные материалы и технологии»

УТВЕРЖДАЮ:

Директор

 И.А. Курзина

« 05 » 11 2024 г.

Рабочая программа дисциплины

Основы информационной безопасности

по направлению подготовки

19.03.01 Биотехнология

Направленность (профиль) подготовки:

«Молекулярная инженерия»

Форма обучения

Очная

Квалификация

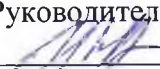
Бакалавр

Год приема

2025

СОГЛАСОВАНО:

Руководитель ОП

 И.А. Курзина

Председатель УМК

 Г.А. Воронова

1. Цель и планируемые результаты освоения дисциплины (модуля)

Целью освоения дисциплины является формирование следующих компетенций:

УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

ОПК-2 Способен осуществлять поиск, хранение, обработку и анализ профессиональной информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий, включая проведение расчетов и моделирование, с учетом основных требований информационной безопасности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИУК-1.1 Осуществляет поиск информации, необходимой для решения задачи;

ИОПК-2.1 Проводит информационный поиск по тематике исследования и осуществляет критический анализ полученной информации.

2. Задачи освоения дисциплины

- обучающиеся должны знать основные документы, регламентирующие организационную безопасность на объекте;
- обучающиеся должны уметь оценивать состояние организационной защиты информации на объекте;
- обучающиеся должны владеть основами организационной и правовой защиты информации, ее современными проблемами и терминологиями.

3. Место дисциплины (модуля) 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

Первый семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются компетенции, сформированные в ходе освоения образовательных программ предшествующего уровня образования.

6. Язык реализации

Русский

7. Объем дисциплины (модуля)

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

– лекции: 8 ч.;

– лабораторные работы: 14 ч.

в том числе практическая подготовка: 14 ч.

Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины (модуля), структурированное по темам

1. Понятие информационной безопасности. Основные составляющие. Важность проблемы;

2. Законодательный уровень информационной безопасности;
3. Информационная война, методы и средства её ведения;
4. Информационная безопасность вычислительных сетей. ИБ при использовании Internet;
5. ИБ компьютеров и компьютерных сетей;
6. Безопасность операционных систем;
7. Компьютерные вирусы и защита от них;
8. Заключение. Подведение итогов курса.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине осуществляется путем проведения опросов, сдаче отчетов по лабораторным работам, выполнения рефератов и фиксируется в форме контрольной точки не менее одного раза в семестр.

Оценочные материалы для проведения промежуточной аттестации 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 первом семестре проводится в защиты реферата по согласованной с преподавателем теме, а также ответы на вопросы. Продолжительность зачета 1 час.

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 электронном университете «Moodle» - <https://moodle.tsu.ru/enrol/index.php?id=8366>
- б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине (<https://www.tsu.ru/sveden/education/eduop/>).
- в) Методические указания по проведению лабораторных работ.
- г) Методические указания по организации самостоятельной работы студентов.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

1. 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 ; [под ред. А. П. Зайцева, А. А. Шелупанова]. - 7-е изд., испр.. - Москва : Горячая линия - Телеком, 2016. - 442 с.: ил. - (Учебник для высших учебных заведений. Специальность)
2. Ищейнов В. Я. Защита конфиденциальной информации : [учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов информатизации"] / В. Я. Ищейнов, М. В. Мещатунян. - Москва : Форум, 2013. - 254 с.: ил., табл. - (Высшее образование)

3. Царегородцев А. В. Методы и средства защиты информации в государственном управлении : учебное пособие / А. В. Царегородцев, М. М. Тараскин. - Москва : Проспект, 2023. - 205 с.: табл.
4. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах : [учебное пособие для студентов высших учебных заведений, обучающихся по направлению 230100 "Информатика и вычислительная техника"] / В. Ф. Шаньгин. - Москва : ИНФРА-М [и др.], 2013. - 591 с.: рис. - (Высшее образование)
5. Галатенко В. А. Основы информационной безопасности : учебное пособие : [для вузов по специальности 351400 "Прикладная информатика"] / В. А. Галатенко. - 4-е изд.. - Москва : Интернет-Университет Информационных Технологий [и др.], 2008. - 205 с.: ил. - (Основы информационных технологий)
6. Основы информационной безопасности : [учебное пособие для студентов вузов, обучающихся по специальностям в области информационной безопасности] / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - М. : Горячая линия - Телеком, 2006. - 544 с.: ил.

б) дополнительная литература:

1. Казарин О. В.. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум / О. В. Казарин, А. С. Забабурин.. - Москва : Юрайт, 2023. - 312 с URL: <https://urait.ru/bcode/513300>
2. Бузов Г. А. Защита информации ограниченного доступа от утечки по техническим каналам / Г. А. Бузов. - Москва : Горячая линия - Телеком, 2019. - 585 с.: ил., табл.
3. Зегжда Д. П. Основы безопасности информационных систем : Учебное пособие для вузов по специальности "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизированных систем" / Д. П. Зегжда, А. М. Ивашко. - М. : Горячая линия - Телеком, 2000. - 449, [3] с.: ил.
4. Айков Д. Компьютерные преступления : Руководство по борьбе с компьютерными преступлениями / Д. Айков, К. Сейгер, У. Фонсторх; Пер. с англ. В. И. Воропаева, Г. Г. Трехалина. - М. : Мир, 1999. - 351, [1] с.: рис. - (Компьютерная безопасность)

в) ресурсы сети Интернет

1. <https://habr.com/ru/hub/infosecurity/> – сайт Хабр, раздел Информационная безопасность и защита данных.

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

- Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook);
- публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).

б) информационные справочные системы:

- Электронный каталог Научной библиотеки ТГУ – <http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system>
- <https://openedu.ru/> – сайт обучающихся курсов ведущих вузов России
- <https://stepik.org/> – сайт онлайн-курсов от ведущих вузов и компаний страны
- ЭБС Лань – <http://e.lanbook.com/>
- Открытый университет Интуит.ру <http://intuit.ru;>
<http://intuit.ru/studies/courses/37/37/info>

14. Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта с перечнем основного оборудования	Адрес (местоположение) учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта (с указанием площади и номера помещения в соответствии с документами бюро технической инвентаризации)
Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Аудитория № 115 Оборудование: Графическая станция, процессор Intel i5, 16Гб оперативной памяти, монитор 24 дюйма Демонстрационный экран Мультимедиа-проектор Учебная мебель: рабочие места по количеству обучающихся (аудиторные столы, стулья); рабочее место преподавателя (стол, стул); аудиторная доска	634050, Томская область, г. Томск, пр-кт Ленина, 36, стр.7 (29 по паспорту БТИ) Площадь 40,9 м²
Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Аудитория № 103а Компьютерный класс: 13 компьютеров ASUS TUF B360-PLUS GAMING, Intel Core i7 8700, 16 ГБ, GeForce RTX 2070 8gb, 1 ТБ Жесткий диск; 240 Гб SSD, Блок питания CHIEFTEC GPC-700S 700 Вт, Корпус Ginzzi A180 без БП, 2. Монитор LG 24MK600M-B 23.8, 3. Клавиатура Logitech K120, Мышь Logitech B100 4. ПО, включающее: 4.1. Windows 7 4.2. Microsoft Office 2010 4.3. Visual Studio 2019 4.4. Visual Studio Code	634050, Томская область, г. Томск, пр-кт Ленина, 36, стр.7 (72 по паспорту БТИ) Площадь 43 м²
Учебная аудитория для самостоятельной работы, индивидуальных консультаций. Аудитория № 121^А Учебная мебель: рабочие места по количеству обучающихся (аудиторные столы, стулья); рабочее место преподавателя (стол, стул)	634050, Томская область, г. Томск, пр-кт Ленина, 36, стр.7 (86 по паспорту БТИ) Площадь 23,8 м²

15. Информация о разработчиках

Гурина Елена Ивановна, доцент кафедры вычислительной математики и компьютерного моделирования ММФ ТГУ.