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

Филологический факультет

УТВЕРЖДЕНО:
Декан
И. В. Тубалова

Рабочая программа дисциплины

Основы информационной безопасности

по направлению подготовки

45.04.03 Фундаментальная и прикладная лингвистика

Направленность (профиль) подготовки:
Компьютерная и когнитивная лингвистика

Форма обучения
Очная

Квалификация
Магистр

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
З.И. Резанова

Председатель УМК
Ю.А. Тихомирова

Томск – 2025

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-3 Способен выбирать оптимальные подходы и методы решения конкретных научных и прикладных задач в области лингвистики и информационных технологий.

ОПК-6 Способен осуществлять эффективное управление разработкой программных средств информационных проектов в сфере своей профессиональной деятельности.

ПК-4 Способен разрабатывать проекты прикладной направленности в области когнитивной и компьютерной лингвистики с применением современных технических средств и информационных технологий, в том числе в области искусственного интеллекта.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-3.3 Способен решать конкретные научные и прикладные задачи в области лингвистики и информационных технологий на основе самостоятельного выбора оптимальных подходов и методов их решения

ИОПК-6.2 Разрабатывает алгоритмы и программы для решения лингвистических и междисциплинарных задач в том числе с применением высокопроизводительных вычислительных технологий

ИОПК-6.3 Разрабатывает и отлаживает программный код, направленный на решение лингвистических и междисциплинарных задач с применением современных языков программирования

ИПК-4.2 Разрабатывает программу действий по решению задач проекта в области когнитивной и компьютерной лингвистики с учетом имеющихся технических средств и информационных технологий, в том числе в области искусственного интеллекта

2. Задачи освоения дисциплины

– овладеть понятийным аппаратом в области информационной безопасности и защиты информации; установление и раскрытие структуры угроз защищаемой информации;

– изучить базовые содержательные положения в области информационной безопасности и защиты информации;

– раскрыть различные формы представления информации в проблемах обеспечения информационной безопасности.

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

Третий семестр, зачет

5. Входные требования для освоения дисциплины

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

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: основные направления обеспечения новых информационных технологий.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 2 з.е., 72 часов, из которых:
-лекции: 6 ч.
-практические занятия: 16 ч.
в том числе практическая подготовка: 16 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Предмет, содержание и задачи курса, его место среди других дисциплин учебного плана. Формы отчетности.

Тема 2. Защита информации как объективная закономерность эволюции постиндустриального общества. Информация и ее роль в современном обществе

Тема 3. Компьютерная система (КС) как объект защиты информации. Угрозы информационной безопасности в компьютерных системах.

Тема 4 Эволюция концепции информационной безопасности в компьютерных системах. Общая характеристика средств и методов защиты информации.

Тема 5. Общая характеристика организационного обеспечения защиты информации. Организационно-правовое обеспечение защиты информации

Тема 6. Охрана объектов КС и средства защиты информации от утечки по техническим каналам. Противодействие подслушиванию. Методы и средства защиты КС от побочных электромагнитных излучений и наводок

Тема 7. Защита КС от несанкционированного вмешательства. Модели управления доступом к информации в КС. Идентификация и аутентификация пользователей и разграничение их доступа к компьютерным ресурсам

Тема 8. Компьютерные вирусы и средства антивирусной защиты. Общие сведения о компьютерных вирусах Профилактика заражения вирусами компьютерных систем

Тема 9. Комплексная защита информации в компьютерных системах (КСЗИ). Концепция создания КСЗИ в КС. Функционирование КСЗИ.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения контрольных работ, тестов по лекционному материалу, практических заданий, выполнения домашних 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/.

Примерный перечень вопросов:

1. Информационные ресурсы, подлежащие защите в сфере финансовой деятельности.
2. Классификация угроз информационной безопасности и их сравнительный анализ.
3. Информационная безопасность в современных условиях хозяйствования. Общегосударственные цели, задачи и методы обеспечения информационной безопасности.
4. Понятия о видах вирусов. Классификация вирусов и угрозы для информационной инфраструктуры хозяйствующих субъектов.
5. Виды возможных нарушений информационной безопасности в сфере финансовой деятельности.
6. Отечественные и международные стандарты обеспечения информационной безопасности.
7. Особенности современной нормативно-правовой и методологической базы обеспечения информационной безопасности.

8. Основные нормативные руководящие документы, касающиеся конфиденциальной информации и государственной тайны, нормативно-справочные документы по обеспечению информационной безопасности применяемые в финансовой деятельности.

9. Общие критерии оценки безопасности информационных систем и технологий ГОСТ 15408, как основа определения требований к обеспечению информационной безопасности.

10. Место информационной безопасности экономических систем в национальной безопасности страны.

11. Цели и задачи обеспечения национальной безопасности. Система целеполагания в структуре государственного и муниципального управления при обеспечении информационной безопасности.

12. Основные положения концепции информационной безопасности. Сравнительная таблица.

13. Государственные информационные ресурсы, подлежащие защите в сфере финансовой деятельности.

14. Взаимосвязь государственных и коммерческих информационных ресурсов (конфиденциальной информации и государственной тайны).

15. Модели безопасности, и их применение.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Зачет во втором семестре выставляется при условии набора 40 баллов за работу в семестре, а также за подготовку и защиту проектной работы, содержащей критический анализ нескольких работ, посвящённых решению какой-либо лингвистической проблемы с применением методов психолингвистики, изученных в ходе курса (проверяется достижение индикаторов – ИОПК-3., ИОПК-6.2, ИОПК-6.3, ИПК-4.2).

Студенты, не набравшие необходимого количества баллов, имеют возможность сдавать зачёт в традиционной форме – по билетам. Каждый билет включает два теоретических вопроса (проверяется достижение индикаторов – ИОПК-3., ИОПК-6.2, ИОПК-6.3, ИПК-4.2).

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 «LMS IDO» - https://lms.tsu.ru/course/view.php?id=00000

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

Текущий контроль:

- Тестовые задания по лекционному материалу.
- Практические задания: подготовка конспектов, участие в дискуссии, представление обзоров статей, подготовка рефератов.
- Терминологический опрос.

Промежуточная аттестация:

- Проектная работа (1 семестр).

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд.,

перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8

– Федоров Н.В. Основы информационной безопасности. Электронный образовательный ресурс. Московский Политех, 2020

– Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3.

б) дополнительная литература:

– Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8

– Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0

– Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с.

в) ресурсы сети Интернет:

– открытые онлайн-курсы

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

– 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/

– ЭБС IPRbooks – http://www.iprbookshop.ru/

в) профессиональные базы данных *(при наличии)*:

– Университетская информационная система РОССИЯ – https://uisrussia.msu.ru/

– Единая межведомственная информационно-статистическая система (ЕМИСС) – https://www.fedstat.ru/

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.

Лаборатории, оборудованные …

Аудитории для проведения занятий лекционного и семинарского типа индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации в смешанном формате («Актру»).

15. Информация о разработчиках

Степаненко Андрей Александрович, старший преподаватель кафедры «Общей, компьютерной и когнитивной лингвистики»