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

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор
_____А. В. Замятин
« 16 » июня 20 23 г.

Рабочая программа дисциплины

Профессиональный перевод специальной литературы

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки / специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2023

Код дисциплины в учебном плане: Б1.О.06.08

СОГЛАСОВАНО:
Руководитель ОП
_____В.Н. Тренькаев

Председатель УМК
_____С.П. Сущенко

Томск – 2023

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

– УК-4 – Способен применять современные коммуникативные технологии, в том числе на иностранных языках, для академического и профессионального взаимодействия.

– ОПК-8 – Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИУК-4.1 Демонстрирует навыки устной и письменной деловой коммуникации на русском и иностранном языках в разных формах в соответствии с поставленными задачами.

ИУК-4.2 Выбирает на государственном и иностранных языках коммуникативно приемлемые стиль делового общения, вербальные и невербальные средства взаимодействия с партнерами.

ИУК-4.3 Использует информационно-коммуникационные технологии при поиске необходимой информации в процессе решения различных коммуникативных задач на государственном и иностранном (ых) языках.

ИОПК-8.1 Осуществляет подбор, изучение и обобщение научно-технической информации, методической информации отечественного и зарубежного опыта по проблемам компьютерной безопасности.

ИОПК-8.2 Составляет научно-технические отчеты, готовит обзоры и публикации по результатам выполненных исследований в области обеспечения безопасности компьютерных систем и сетей.

2. Задачи освоения дисциплины

- совершенствование иноязычной компетенции в различных видах речевой деятельности (аудировании, говорении, чтении, письме, переводе) в ситуациях академического и профессионального взаимодействия;
- совершенствование коммуникативной компетенции, необходимой для иноязычной деятельности в соответствии с конкретными ситуациями, условиями и задачами академического и профессионального общения;
- развитие умений и навыков аннотирования и реферирования профессиональной литературы, цитирования и оформления ссылок в научных работах на английском языке;
- формирование и развитие навыков письменного перевода профессиональной литературы;

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в модуль «Специализация».

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

Пятый семестр, зачет
Шестой семестр, зачет с оценкой

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Иностранный язык.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 6 з.е., 216 часов, из которых:
-практические занятия: 128 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Введение в криптографию. Безопасность данных
Освоение терминов и терминологического словаря по теме «Криптография»

Тема 2. Поточное шифрование
Освоение терминов и терминологического словаря по теме «Поточное шифрование»
Тема 3. Стандарт шифрования данных (DES)
Освоение терминов и терминологического словаря по теме «Стандарт шифрования данных (DES)»
Тема 4. Расширенный стандарт шифрования данных (симметричный алгоритм блочного шифрования)
Освоение терминов и терминологического словаря по теме «Симметричный алгоритм блочного шифрования)»
Тема 5. Блочные шифры
Освоение терминов и терминологического словаря по теме «Блочные шифры»
Тема 6. Введение в криптографию с отрытым ключом
Освоение терминов и терминологического словаря по теме «Криптография с отрытым ключом»
Тема 7. Криптосистема с открытым ключом (The RSA Cryptosystem)
Освоение терминов и терминологического словаря по теме «The RSA Cryptosystem»
Тема 8. Криптосистема с открытым ключом, основанная на задаче дискретного логарифмирования
Освоение терминов и терминологического словаря по теме «Задача дискретного логарифмирования»
Тема 9. Криптосистема на основе эллиптических кривых
Освоение терминов и терминологического словаря по теме «Эллиптические кривые»
Тема 10. Цифровые подписи
Освоение терминов и терминологического словаря по теме «Цифровые подписи»
Тема 11. Хеш функции/ Функции хеширования
Освоение терминов и терминологического словаря по теме «Хеш функции»
Тема 12. Коды проверки подлинности сообщение
Освоение терминов и терминологического словаря по теме «Коды проверки подлинности сообщение»

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения контрольных работ, выполнения домашних заданий, мониторинга СРС, опроса (индивидуального, комбинированного, взаимного), собеседования, групповых учебных дискуссий, Выполнение этих работ является обязательным для всех обучающихся, а результаты являются основанием для выставления оценок (баллов) текущего контроля. Результаты текущего контроля фиксируются в форме контрольной точки не менее одного раза в семестр.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Промежуточная аттестация обучающихся осуществляется в форме зачета в 5 семестре.

Зачёт состоит из устной части. Устная часть состоит из презентации академического характера и обсуждении ряда профессиональных тем.

Промежуточная аттестация обучающихся (Зачет с оценкой) осуществляется в форме зачета в 6 семестре.

Зачёт состоит из письменной и устной частей. Письменная часть представлена написание творческой работы академического характера (реферат, доклад и т.п.). Устная часть состоит из презентации академического характера и обсуждении ряда профессиональных тем.

Результаты дифференцированного зачета определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и являются средним арифметическим баллов, полученных за все задания в рамках итоговой аттестации.

Оценка «отлично» выставляется, если студент уверенно владеет различными средствами устной и письменной коммуникации, лексическим и грамматическим материалом; допускает незначительные (не более 2х грамматических и 3-4х лексических; продолжительность речи не менее 3х минут) ошибки в речи, которые не затрудняют коммуникацию.

Оценка «хорошо» выставляется, если студент владеет различными средствами устной и письменной коммуникации, лексическим и грамматическим материалом; допускает незначительные (не более 4х грамматических и 5-6ти лексических; продолжительность речи не менее 3х минут) ошибки в речи, которые не затрудняют коммуникацию; студент способен корректировать свое коммуникативное поведение.

Оценка «удовлетворительно» выставляется, если студент неуверенно и не в полном объеме владеет средствами устной и письменной коммуникации, не демонстрирует разнообразие в использовании лексического и грамматического материала; студент с трудом способен корректировать свое коммуникативное поведение.

Оценка «неудовлетворительно» выставляется, если студент не демонстрирует владение средствами устной и письменной коммуникации, лексическим и грамматическим материалом; многочисленные ошибки в речи затрудняют коммуникацию и искажают смысл сказанного; студент не способен корректировать свое коммуникативное поведение.

Типовые задания для проведения текущего контроля успеваемости по дисциплине.

Task 1. Complete these sentences with the link words from the box**.**

However / Moreover/ Because /Also/ However/ for example

In practice, in particular for encrypting computer communication on the Internet, block ciphers are used more often than stream ciphers.
_1_ stream ciphers tend to be small and fast, they are particularly relevant for applications with little computational resources, _2__ for cell phones or other small embedded devices. A prominent example for a stream cipher is the A5/1 cipher, which is part of the GSM mobile phone standard and is used for voice encryption. _3_ stream ciphers are sometimes _4_ used for encrypting Internet traffic, especially the stream cipher RC4.

Traditionally, it was assumed that stream ciphers tended to encrypt more efficiently than block ciphers. *Efficient* for software-optimized stream ciphers means that they need fewer processor instructions (or processor cycles) to encrypt one bit of plaintext. For hardware-optimized stream ciphers, *efficient* means they need fewer gates (or smaller chip area) than a block cipher for encrypting at the same data rate. _5_ modern block ciphers such as AES are also very efficient in software. __6_ for hardware, there are also highly efficient block ciphers, such as PRESENT, which are as efficient as very compact stream ciphers.

Task 2. Read these sentences and translate the Russian words and phrases into English.

1. **(Так как)** encryption and decryption functions are both simple additions modulo 2, we can (**изобразить)** the basic operation of a stream cipher as shown in Fig.
2. **Block ciphers** encrypt an (**целый**) block of plaintext bits (**одновременно)** with the same key. **Stream ciphers** encrypt bits **(отдельно)**.
3. **(Необходимо отметить)** we use a circle with an addition sign as the symbol for modulo 2 addition.
4. **(Что касается)** the substitution cipher, **(можно)** also use letter frequency analysis.
5. **(Требуется некоторое усилие**) to find the inverse (usually employing the Euclidean algorithm).
6. **(Однако),** there is an easy way of telling whether an inverse for a given element a exists or not.
7. We can (**добавить)** and (**умножить)** any two numbers and the (**результат)** is always in the ring. A ring (**говорят/считают)** to be closed.
8. However, (**с точки зрения математики)** it does not matter which member of an equivalent class we use.
9. To make computations with letters more (**осуществимый)**, we can **(присвоить)** each letter of the alphabet a number.
10. **(Необходимо сделать акцент/подчеркнуть)** that Moore's Law is an exponential function.

Типовые задания для проведения промежуточной аттестации по дисциплине

Task 1. Study the content of the table:

a. First study main issues of any research paper. (left column)
b. Then highlight the issues (right column) of the paper you have read. (Any research paper recommended by your supervisors)

Main Issues of a research paper	**Highlight the following issues after reading a research paper**
Title	Introduce the title of the paper
Author(s)	Introduce the authors of the paper (what university/institute/laboratory they come from)
Subject	What is the subject of their study(research)?
Structure Like any other research paper, is supposed to consist of the following sections: • **Title;**	What sections does the paper (you've read) include? •

• **Abstract;(with key words)** • **Introduction;** • **Main body;** • **Conclusions;** • **Acknowledgements;** • **References.** However, the number of sections and their names can vary in different journals.	• • **Etc.**
Introduction • **Background to the topic** (Readers get familiar with the general context) • Accepted ***state of the art*** **plus** ***problem*** to be resolved (the gap that the authors want to fill) • What is the problem? • Are there any existing solutions (i.e. in the literature)? • Which solution is the best?	State the problem of this study/research. (Use Pr. Simple) State the main findings of this study/research. (Use Pr. Perfect)
Grammar Tenses: **Present Simple** is generally used to begin the Introduction in order to describe the general background context, i.e. what is known already **Present Perfect** is used to show how the problem has been approached	Find verbs in Introduction and identify their Gr. Tenses.

Get prepared to speak about the problem you are going to study/investigate in your course work/project. (Preliminary Speaking). These questions might help you.

1. (In) What field are you going to do research?
2. What will your course work be entitled?
3. What problem are you going to study/investigate?
   What is the gap you are going to fill in? (In the field of your study/investigation)
4. What is the background of the problem?
   What is state-of –the-art study/research in this field?
5. What is the aim/purpose of your study/investigation? What do you want to achieve?
6. Is the subject of the paper (you have read) **relevant** to the problem you study/investigate?

Task 2. There are several ways of encrypting long plaintexts with a block cipher. Describe each mode of operation (in the right column of the table).

Modes of Operation	Main features of modes
• ***Output Feedback Mode (OFB)*** • ***Cipher Feedback Mode (CFB)*** • ***Counter Mode (CTR)*** • ***Galois Counter Mode (GCM)***	

2. Темы для **презентации** академического характера определяются студентами самостоятельно, исходя из темы их курсовой работы.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle»

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине (Приложение 1).

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

- Christof Paar, Jan Pelzl Understanding Cryptography. ATextbook for Students and Practitioners, Springer, 2010 г. 372 с.

б) дополнительная литература:

- Matt Bishop, Introduction to Computer Security, Addison – Wisley, 2004 г., 747 с.
- Mark Stamp, Richard M. Low Breaking Ciphers in the Real World, John Wiley & Sons, 2007 г., 401 с.
- Поленова А.Ю., Числова А.С. A Complete Guide to Modern Writing Forms. Современные форматы письма в английском языке: учебник Москва: ИНФРА-М: Академцентр, 2012 г., 160 с.

в) ресурсы сети Интернет:

1. Электронная библиотека (репозиторий) ТГУ [Электронный ресурс] / Электронная библиотека (репозиторий) ТГУ : [сайт]. – [Томск, 2011–2016]. – URL: http://vital.lib.tsu.ru/vital/access/manager/Index.
2. Система дистанционного обучения ТГУ LMS Moodle [Электронный ресурс] / https://moodle.tsu.ru/
3. Youtube (видеохостинг) [Электронный ресурс] / http://youtube.com
4. 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

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.

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

15. Информация о разработчиках

Бутузова Т.В.: старший преподаватель кафедры английского языка естественнонаучных и физико-математических факультетов ФИЯ