

Программа учебной дисциплины «Английский язык для профессионального общения»

Утверждена

Академическим советом ООП

Протокол № от «__» _____ 20__ г.

Авторы	Антонова М.Б., Бакулев А.В., Прилипко Е.В.
Число кредитов	3
Контактная работа (час.)	52
Самостоятельная работа (час.)	56
Курс	4, специалитет
Формат изучения дисциплины	Без использования онлайн курса

I. ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ

Целью освоения дисциплины «Английский язык для профессионального общения» является формирование профессионально ориентированной иноязычной коммуникативной компетенции в английском языке в области «Компьютерная безопасность» на уровнях B2+ – C1 по шкале CEFR.

В результате освоения дисциплины студент должен:

знать:

- особенности профессионального дискурса области «Компьютерная безопасность»;
- требования к речевому и языковому оформлению устных и письменных высказываний научно-исследовательской тематики с учетом специфики англоязычного академического дискурса и профессиональной сферы;
- терминологию профессиональной области;

уметь:

- порождать объемные письменные тексты (1500 – 2500 слов) – отчеты об исследовательском проекте в формате научной статьи;
- правильно оформлять внутритекстовые ссылки, а также список использованной литературы;
- воспринимать на слух высказывания на профессиональную тематику разного темпа и сложности;
- читать объемные тексты профессионально ориентированного характера;
- подготовить тезисы устного сообщения (презентации) по проекту;
- подготовить слайды устного сообщения по проекту;
- делать сообщения на профессиональную тему с элементами повествования, описания и рассуждения с учетом требований академического дискурса;
- комментировать цифровые или визуальные данные, представленные на слайде;
- начинать, вести, поддерживать и заканчивать диалог, используя при необходимости стратегии компенсации сбоя в процессе коммуникации (переспрос, перефразирование и т.д.);

- отвечать на вопросы коллег по тематике, представленной в проекте на защиту / в выступлении на круглом столе, конференции и т.д;
- понимать звучащую речь в пределах литературной нормы в академической и профессиональной среде;
- понимать вопросы коллег по презентуемой теме;

владеть:

- навыками самостоятельного поиска и систематизации информации с использованием специальных источников профессионального и академического характера;
- навыками быстрого просмотрового чтения объемных академических текстов профессиональной направленности, с выделением важной информации и умением определить актуальность проблемы;
- навыками работы с онлайн-библиотеками и базами данных, в том числе посредством использования онлайн-подписок НИУ ВШЭ;
- навыками публичного выступления с использованием слайдов;
- навыками ведения дискуссии на общие и профессиональные темы с выражением собственного мнения и подкреплением его аргументами;
- компенсаторными стратегиями, помогающими преодолеть затруднения в коммуникации, вызванные объективными и субъективными причинами.

Дисциплина «Английский язык для профессионального общения» связана с дисциплиной «Иностранный язык», читаемой на 1 – 2 курсах, с дисциплинами специализации «Компьютерная безопасность», реализуемых на разных ступенях как на русском, так и на английском языке, а также научно-исследовательским и проектным семинарами.

Пререквизит: владение студентами английским языком на уровне не ниже В2.

II. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Тема 1. Общая характеристика целей и задач курса. Проблемы фундаментальных исследований и практических разработок в области информационных технологий и компьютерной безопасности. Прикладной характер компьютерной безопасности. Просмотр и обсуждение видеопрезентации по указанной тематике.

Тема 2. Проведение исследований в области информационных технологий и компьютерной безопасности. Академический дискурс как средство представления результатов научных разработок. Устный и письменный академический дискурс. Научная статья как один из форматов представления результатов научных изысканий. Жанро-стилевые особенности англоязычной научной статьи.

Тема 3. Научно-исследовательская работа студентов в области информационных технологий и компьютерной безопасности. Обсуждение возможных тем индивидуальных и групповых проектов. Отчет по проекту (Project Proposal) в формате научной статьи как форма письменной отчетности по планируемому и/или достигнутым результатам проекта.

Тема 4. Основные понятия компьютерной безопасности. Критерии уровня информационной безопасности. Средства защиты информации. Подбор, чтение и обсуждение научной статьи по указанной проблематике.

Тема 5. Целеполагание в научном исследовании. Контекст научного исследования. Постановка цели и исследовательских вопросов. Введение как часть научной статьи. Содержательные, композиционные и языковые особенности введения.

Тема 6. Криптография и стеганография как средства защиты информации. Подбор, чтение и обсуждение научной статьи по указанной тематике. Обзор литературы как компонент научной статьи и манифестация научной квалификации и этики автора. Понятия авторского права и плагиата.

Тема 7. Квантовая криптография как средство информационной безопасности. Поляризация. Поляризационные фильтры. Подбор, чтение и обсуждение статьи по указанно тематике. Составление примерного плана обзора литературы для отчета по проекту.

Тема 8. Методы исследования в области информационных технологий и компьютерной безопасности. Раздел «Методы» как компонент научной статьи. Обсуждение различных методов исследования в указанной области применительно к исследовательским проектам, выполняемым студентами.

Тема 9. Новые проблемы информационной безопасности в контексте глобальных рисков и угроз. Просмотр и обсуждение видеолекции по указанной проблематике. Раздел «Планируемые/достигнутые результаты» как компонент научной статьи. Содержательные, композиционные и языковые особенности данного раздела.

Тема 10. Разделы «Заключение» и «Аннотация» научной статьи. Содержательные, композиционные и языковые особенности данных разделов. Обсуждение планируемых результатов исследовательских проектов, выполняемых студентами.

Тема 11. Редактирование и форматирование научной статьи. Цитирование и список источников. Стили оформления внутритекстовых ссылок и списка литературы. Устная презентация и научная дискуссия по проблематике исследовательского проекта. Жанро-стилевые особенности устной презентации в академическом дискурсе. Правила оформления слайдов. Стратегии и тактики ведения научной дискуссии, в том числе ответов на неудобные и неудачные вопросы.

III. ОЦЕНИВАНИЕ

Оценка по курсу «Английский язык для профессионального общения» рассчитывается по следующей формуле:

$$O_{\text{результатирующая}} = O_{\text{накопленная}} * 0,6 + O_{\text{экзамен}} * 0,4$$

Накопленная оценка формируется следующим образом:

$$O_{\text{накопленная}} = O_{\text{ауд}} * 0,3 + O_{\text{тесты}} * 0,3 + O_{\text{письм.работы}} * 0,3$$

Аудиторная работа предполагает активное участие в обсуждениях, развернутые монологические высказывания, суждения и комментарии, релевантные тематике обсуждения, комментарии в рамках само- и взаимооценивания.

Тесты представляют собой мини-контрольные работы и включают в себя задания по аудированию и/или чтению профессионально ориентированных текстов, а также тесты по профессионально ориентированной лексике.

Письменные работы включают написание разделов отчета по проекту в формате научной статьи и их взаимооценивание.

Оценка за экзамен рассчитывается следующим образом:

$$O_{\text{экз}} = O_{\text{письм. часть}} * 0,5 + O_{\text{устн. часть}} * 0,5$$

Письменная часть представляет собой отчет по исследовательскому проекту в формате научной статьи объемом 1500 – 2000 слов. В случае выполнения группового проекта объем может быть увеличен до 2500 слов. Письменная часть сдается студентами в бумажном (лично преподавателю) и электронном виде (на электронную корпоративную почту преподавателя) за две недели до устной части. Устная часть – защита исследовательского проекта перед экзаменационной комиссией, в которую входит преподаватель дисциплины и преподаватель кафедры компьютерной безопасности.

В случае, если студент не сдал письменную часть экзамена за две недели до устной части, он к устной части не допускается и получает неудовлетворительную результирующую оценку по дисциплине даже при высокой накопленной оценке. Это единственный блокирующий элемент курса. Других блокирующих элементов не предусмотрено.

Студент, получивший по дисциплине результирующую неудовлетворительную оценку, имеет право на две пересдачи. Первая пересдача проходит в формате экзамена. Экзаменаторы учитывают накопленную оценку.

В случае получения неудовлетворительной оценки из-за блокирующего элемента студент обязан сдать письменную часть за три дня до пересдачи. В противном случае блокирующий элемент вновь «срабатывает», и студент не допускается к устной части, получая неудовлетворительную оценку.

Вторая пересдача принимается комиссией в составе не менее трех человек в формате экзамена. При этом члены комиссии имеют право не учитывать накопленную оценку. Если на первой пересдаче студент получил неудовлетворительную оценку из-за блокирующего элемента, он должен предоставить письменную часть за три дня до заседания комиссии. В противном случае студент не допускается к устной части и получает неудовлетворительную оценку.

IV. ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ

1. Give English equivalents for the following terms.

1) требование безопасности

2) объект оценки

3) административно-правовая основа

4) несанкционированное разглашение

5) целостность

2. Read the cover letter and use the verbs in parentheses in the correct form.

As mentioned on the telephone to your administrative secretary, I would be interested in an internship in your antivirus design laboratory. I (graduate) in Computer Science at the University of Oregon in 2014, and I (obtain) a Master's in Cyber Security the following year in Karlsruhe. I then (work) on two major projects using neural networks. The first one (base) in Shanghai and the second in Beijing.

I (be) now back at the University of Oregon where for the last three months I (be) an assistant professor. So far I (design) three different virus detection software applications, and I (work) currently on an antivirus system to protect the University's LMS. Over the last three years I also (gain) considerable experience in other aspects of IT and cyber security as I (attend) several congresses on such areas as artificial intelligence and Internet security, new authentication methods, and security and ethics in bioinformatics. I also (give) a series of workshops on these subjects here in Oregon, the last of which (hold)be held at the end of this month.

My native language (be) Chinese, but I also (speak) fluent German as I (do) a language course while I (be) in Karlsruhe for my Master's. I (spend) a considerable amount of time here in the USA, so English (be) basically my second language.

3. Arrange the parts of an introduction in the right order. Put the correct numbers next to the number symbol (#).

A. Unfortunately, the UK's 2016 report on the National Cyber Security Strategy stated that smaller businesses' "awareness of the personal relevance of the cyber risk is patchy" (UK Government, 2016b). Individual consumers have shown an increased awareness of security, yet small organisations, also treated as consumers by their service providers, are lagging behind in their uptake of the measures that the UK government has identified as a minimum for reducing the risks they feel all UK Internet users face (UK Government, 2014). # _____

B. We report results of an empirical study that evaluated SSITU technology use, with respect to their ability to apply security measures, within a broader ecosystem of small-scale cyber security stakeholders in the UK. The study was motivated by a lack of available data about the environment in which these small organisations make their cyber security decisions, which makes the design of sector-specific security measures challenging. # _____

C. In 2011 the UK government released a National Cyber Security Strategy (UK Government, 2011). From the outset this mentions enhancing the security of consumers and smaller organisations as part of a broader aim to support economic growth. Of course, the need for cyber security in smaller

organisations is by no means a new problem. In 1996, with the growth of personal computing, Carroll (Carroll, 1996) wrote: # _____

D. The structure of the remainder of this paper is as follows. Section 2 describes the methodology used in the survey. Alongside the infrastructure (Section 3) and system interactions (Section 5) that make up a typical cyber security discussion, in Section 4 we have included the digital footprint of a SSITU – the scope of their virtual presence – as a vital element of the decision making process. We draw our conclusions in Section 6. # _____

E. “Most books on security were written for big-time users like banks and government agencies where enormous sums of money, or state secrets were at stake. Most PC systems could never meet the security requirements of these mainframe and minicomputer systems. And if they could, the average business or professional person could neither afford them nor be bothered maintaining them.” (Carroll, 1996) # _____

F. If attempts to increase the level of cyber security awareness in small organisations have not resulted in mitigated risks one might ask: If a SSITU has justified investing in cyber security, what constraints within their IT system limit their decisions? To this end, the paper focuses on system and cyber security architectures, drawing comparisons between the systems implemented and common corporate cyber security practices. # _____

G. In the United Kingdom (UK), small companies (defined as employing fewer than 50 people) account for 99.3% of all private sector businesses and 48% of employment (UK Government, 2015a), 88% of charities in the UK (approximately 145,000) are also classed as micro, small or medium by the UK Charity Commission (UK Government, 2016a), and 92% of the population is online. Despite this, small-scale IT users (SSITUs – defined in Section 2) do not typically spring to mind when one considers the term cyber security. # _____

From the journal Computers and Security

V. РЕСУРСЫ

1. Основная литература

Барановская, Т.А. Английский язык для академических целей. English for academic purposes: учеб. пособие для бакалавриата и магистратуры / Т.А. Барановская, А.В. Захарова, Т.Б. Поспелова, Ю.А. Суворова ; под ред. Т. А. Барановской. — М. : Издательство Юрайт, 2017 (или более поздние издания). — 198 с. — URL: www.biblio-online.ru/book/F9CC72D1-7EC2-40A7-9772-9ABD7C109B07. – ЭБС «Юрайт»

Сомко А.С. Профессиональный иностранный язык для специалистов в области компьютерной безопасности / А.С. Сомко, Е.А. Федорова. – СПб: Университет ИТМО, 2016. - 33 с. – URL: <https://books.ifmo.ru/file/pdf/1992.pdf> (книга выложена в открытом доступе на сайте ИТМО)

Стогниева, О.Н. Английский язык для ИТ-направлений. English for information technology: учеб. пособие для академического бакалавриата / О.Н. Стогниева. — М.: Издательство Юрайт, 2017 (или более поздние издания). — 143 с. — URL: www.biblio-online.ru/book/A1CCD80D-BA4D-4597-82A2-D5AE221B4618. – ЭБС «Юрайт»

2. Дополнительная литература

Буренко, Л.В. First Steps in Scientific Communication: Учебное пособие / Л.В. Буренко, В.П. Овчаренко, Л.К. Сальная. – Таганрог: Южный федеральный университет, 2016. – 78 с. – URL: <http://proxylibrary.hse.ru:2060/catalog/product/996389> - ЭБС “Znanium.Com”

Deibert, Ronald. Access Denied: The Practice and Policy of Global Internet Filtering. / Ronald Deibert, John Palfrey, Ratal Rohozinski, and Jonathan Zittrain (eds). - The MIT Press, 2008. URL: <http://common.books24x7.com/toc.aspx?bookid=26545>. – Books24X7 Database

Ulsch, MacDonnell. Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks / Mac Donnell Ulsch. – John Wiley & Sons, Incorporated, 2014. – URL: <https://ebookcentral.proquest.com/lib/hselibrary-ebooks/detail.action?docID=1742833>. – ProQuest Ebook Central Database

3. Программное обеспечение

№ п/п	Наименование	Условия доступа
1.	Microsoft Windows 7 Professional RUS Microsoft Windows 10 Microsoft Windows 8.1 Professional RUS	Из внутренней сети университета (договор)
2.	Microsoft Office Professional Plus 2010	Из внутренней сети университета (договор)

4. Профессиональные базы данных, информационные справочные системы, интернет-ресурсы (электронные образовательные ресурсы)

№ п/п	Наименование	Условия доступа
<i>Профессиональные базы данных, информационно-справочные системы</i>		
1.	Консультант Плюс	Из внутренней сети университета (договор)
2.	Электронно-библиотечная система Юрайт	URL: https://biblio-online.ru/
3.	Электронно-библиотечная система Znanium.com	URL: http://znanium.com/
4.	Электронно-библиотечная система Books24x7	URL: https://library.books24x7.com
5.	Электронно-библиотечная система ProQuest Ebook Central	URL: https://ebookcentral.proquest.com/
6.	Электронная база данных зарубежной периодики IEEE Xplore	URL: https://ieeexplore.ieee.org
7.	Электронная база данных зарубежной периодики ScienceDirect	URL: https://www.sciencedirect.com/
<i>Интернет-ресурсы (электронные образовательные ресурсы)</i>		
1.	Платформа TED	URL: https://www.ted.com
2.	Видеохостинг YouTube	URL: https://www.youtube.com
3.	Ресурсы Центра академического письма НИУ ВШЭ	URL: https://academics.hse.ru/awc/resource
4.	Ресурс Манчестерского университета Academic Phrasebank	URL: http://www.phrasebank.manchester.ac.uk/

5. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине обеспечивают использование и демонстрацию тематических иллюстраций, соответствующих программе дисциплины в составе:

- ПЭВМ с доступом в Интернет (операционная система, офисные программы, антивирусные программы);
- мультимедийный проектор с дистанционным управлением.