Программа учебной дисциплины«Английский язык для профессионального общения»

Утверждена

Академическим советом ООП

Протокол № от «__»_____20__ г.

Авторы	Голечкова Т.Ю., Прогонова Е.В.
Число кредитов	3
Контактная работа (час.)	52
Самостоятельная работа (час.)	62
Курс	3, 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:

- 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 B2.

II. Содержание УЧЕБНОЙ ДИСЦИПЛИНЫ

Тема 1. Programming. Парадигмы программирования, их характеристики, функциональность. Языки программирования, типы, характеристики, функциональность, применение. Освоение лексического материала. Формат краткого сообщения по научной статье.
Тема 2. The Internet. История создания интернета. Открытия и разработки в области информационных технологий, приведшие к созданию всемирной паутины во второй половине 20в. Освоение тематического и лексического материала. Формат краткого сообщения по научной статье.
Тема 3. Information security. Безопасность пользователей в интернете. Основные типы кибер преступлений и методы их совершения. Способы обеспечения необходимой защиты в интернете. Освоение лексического материала. Формат краткой научной презентации. Подготовка материала, подготовка слайдов. Ответы на вопросы. Формат научных дебатов. Аргументация высказываний, анализ источников информации.
Тема 4 Artificial Intelligence. Искусственный интеллект, определение, типы. нейронные сети, типы. использование в различных сферах применения искусственного интеллекта. Экспертные системы, принцип работы, применение. Роботы, применение, принцип работы. Формат описания процесса, диаграммы. Формат краткой научной презентации.
Тема 5. Careers in IT. Направления работы в сфере IT, специальности, требуемые профессиональные навыки. Составление резюме. Формат бизнес презентации.
Тема 6. Projects in IT. Формулирование задачи проекта, стадии выполнения проекта, анализ предыдущих работ, анализ возможных методов и техник, анализ полученных результатов. Формат краткой научной презентации.

III ОЦЕНИВАНИЕ

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

$$\mathbf{О_{результирующая} = О_{накопленная} * 0,6 + О_{экзамен} * 0,4}$$

Накопленная оценка формируется следующим образом:

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

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

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 краткое реферирование научных статей и их взаимооценивание.

Оценка за экзамен рассчитывается следующим образом:

$$\mathbf{О_{экз} = О_{презентация} * 0,5 + О_{ответы\ на\ вопросы} * 0,5}$$

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

Вторая пересдача принимается комиссией в составе не менее трех человек в формате экзамена. При этом члены комиссии имеют право не учитывать накопленную оценку.

IV ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ

1. Give English equivalents for the following terms.

1) требование безопасности

_____

2) уязвимость

_____

3) нарушение авторских прав

_____

4) нарушение целостности информации

_____

5) нарушитель _____

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. Make a plan for rendering this article. Highlight key ideas, use Reporting Verbs to render this article.

Encryption Backdoors

By John P. Mello Jr. Sep 5, 2018 5:00 AM PT

Strong encryption can be a threat to law enforcement and national security, the governments of the United States, United Kingdom, Canada, Australia and New Zealand said in a statement issued Sunday.

"The increasing use and sophistication of certain encryption designs present challenges for nations in combating serious crimes and threats to national and global security," maintained the countries, which are known as the "Five Eyes" based on an agreement they entered to cooperate on signal intelligence.

"Many of the same means of encryption that are being used to protect personal, commercial and government information are also being used by criminals, including child sex offenders, terrorists and organized crime groups to frustrate investigations and avoid detection and prosecution," they added.

The statement sets out three principles the nations agreed to abide by when dealing with encryption within their jurisdictions:

- Access to lawfully obtained data shall be a mutual responsibility of all stakeholders -- government, carriers, device manufacturers and over-the-top service providers.
- All governments should ensure that assistance requested from providers is underpinned by the rule of law and due process protections.
- Information and communications technology service providers should voluntarily establish lawful access solutions to their products and services.

Do It or Else

Whether compliance with the lawful access demands of the Five Eyes will be voluntary for long remains to be seen, especially in light of the final paragraph in the statement:

"Should governments continue to encounter impediments to lawful access to information necessary to aid the protection of the citizens of our countries, we may pursue technological, enforcement, legislative or other measures to achieve lawful access solutions."

That language reeks of Australia, noted Nate Cardozo, a senior staff attorney at the Electronic Frontier Foundation, a digital privacy advocacy group in San Francisco.

For more than a year, Australia has been mulling over legislation aimed at regulating encryption within its borders.

"Australia is looking to lead the charge against security, privacy and technology," Cardozo told TechNewsWorld. "It believes itself to be in a security crisis, and since it doesn't have much hope of getting tech investment, it's more likely to do something to the tech sector."

Good Guys With Bad Encryption

Forcing companies to provide governments access to encrypted data likely will be a losing proposition, both for the governments and the people they're trying to protect.

"Bad guys will just be chased to places where strong encryption is available, and good citizens won't have the opportunity to use the best possible encryption," argued Balakrishnan Dasarathy, information assurance program chair at the University of Maryland University College in Largo, Maryland.

"Good guys will follow the rules and not have all the best technology," he told TechNewsWorld.

Although law enforcement has complained about encryption, the technology has failed to prevent it from getting what it wanted in the past.

"Time and time again law enforcement gets what it needs without backdoors," EFF's Cardozo observed.

"Backdoors make law enforcement's job easier at the cost of all our security," he continued. "Encryption is a magic bullet only if you use it absolutely correctly, which literally no one does."

Backdoors Unnecessary

There is no way to expose data to friendly spy agencies without also risking exposure of this data to not-so-friendly entities, maintained Craig Young, a computer security researcher at Tripwire, a cybersecurity threat detection and prevention company in Portland, Oregon.

"The truth of the matter is that backdoors simply make the process effortless and can enable bulk data collection without individualized suspicion of wrongdoing," he told TechNewsWorld.

"Even without backdoors added into communication protocols, intelligence agencies and law enforcement should generally have other tools at their disposal to gain access to endpoints and thereby circumvent the need to break any encryption," said Young.

"Listening devices, hardware key loggers, and malware can all effectively defeat end-to-end encryption for an individual without adding risk to the general public," he explained.

Encryption is either strong or it is broken, without much of any room for middle ground, Young contended.

Encryption Horse Out of Barn

Backdoors create great risk to the security of data, noted Young.

"Widespread deployment of any backdoor creates tremendous risk if a third party were ever to gain access either through legal channels or reverse engineering," he pointed out.

"Anything you do for the good guys will get into the hands of the bad guys also," said UMUC's Dasarathy. "It's only a matter of time. You're only kidding yourself if you think otherwise."

The Five Eyes' attempt to curb the trend toward encryption may be based on an antiquated notion.

"The cat is very much out of the bag on strong encryption," Tripwire's Young said. "Anyone with an inkling of technology prowess is capable of building their own private communication scheme."

Backdoor keys almost inevitably would fall into the wrong hands, Cardozo suggested. Further they wouldn't enable the good guys to get the bad guys they're after.

Applications with strong encryption would appear online, be downloaded and sideloaded onto phones, he said.

"It takes only the tiniest bit of technical sophistication to install an app, and that's all it will take to get around a backdoor," Cardozo noted.

What's more, "any attacker who is sophisticated enough to recognize a listening device or a physical implant from the NSA is certainly not going to rely on a public communication infrastructure without strong end-to-end encryption," Young noted.

Public Distrust of Government

If the Five Eyes decide to make good on their threat to force the use of backdoors in encrypted products, they may find themselves at odds with a lot of their citizens.

Fewer than half (41 percent) of the 3,000 consumers polled in the U.S., UK and Germany believed laws that provided government access into encrypted personal data would make them safer from terrorists. The survey was conducted last year by Salt Lake City-based Venafi, maker of a platform to protect encryption keys.

Skepticism of government was high in general, with nearly two-thirds (65 percent) suspecting their governments abused their powers to access the data of citizens. That number was even higher in the United States, where 78 percent of respondents held that belief.

"Giving governments access to encryption will not make us safer from terrorism -- in fact, the opposite is true," said Venafi CEO Jeff Hudson.

"Most people don't trust the government to protect data, and they don't believe the government is effective at fighting cybercrime," he added. "It's ironic that we believe we would be safer if governments were given more power to access private encrypted data, because this will undermine the security of our entire digital economy." ECT

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 Donnel 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
	Профессиональные базы данных, информационно-справочные системы	
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/
	Интернет-ресурсы (электронные образовательные ресурсы)	
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.