

**К ВОПРОСУ О ПОВЫШЕНИИ ОСВЕДОМЛЕННОСТИ СТУДЕНТОВ  
ТРАНСПОРТНЫХ УНИВЕРСИТЕТОВ РОССИЙСКОЙ ФЕДЕРАЦИИ И  
РЕСПУБЛИКИ БЕЛАРУСЬ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Матвеева Н.В.<sup>1</sup>, Шатров С.Л.<sup>2</sup>**

*<sup>1</sup>-Российский университет транспорта (МИИТ)*

*<sup>2</sup>-Белорусский государственный университет транспорта, г. Гомель, Республика Беларусь*

**Аннотация.** В статье дается представление о текущем состоянии преподавания и изучения тем, связанных с информационной безопасностью, в рамках курса профессионально-ориентированного английского языка (ESP) в технических университетах Российской Федерации и Республики Беларусь. Исследование было проведено на базе Российского университета транспорта, Москва, и Белорусского государственного университета транспорта, Гомель. В результате тематического анализа Свода знаний по кибербезопасности (СУВоК) и материалов Международной федерации по обработке информации (IFIP) были выявлены актуальные темы. Произведенный анализ учебного материала по английскому языку с точки зрения наличия тем, связанных с информационной безопасностью, показал, что в учебных материалах затрагивается менее 50% актуальных вопросов. Даны рекомендации по совершенствованию учебно-воспитательного процесса.

**Ключевые слова:** информационная безопасность, курс профессионально ориентированного английского языка, университет, учебник, СУВоК, IFIP.

**ON THE ISSUE OF RAISING AWARENESS OF STUDENTS OF TRANSPORT  
UNIVERSITIES OF THE RUSSIAN FEDERATION AND THE REPUBLIC OF BELARUS  
IN THE FIELD OF INFORMATION SECURITY**

**Matveeva N.V.<sup>1</sup>, Shatrov S.L.<sup>2</sup>**

*<sup>1</sup>-Russian University of Transport (MIIT)*

*<sup>2</sup>-Belarusian State University of Transport, Gomel, Republic of Belarus*

**Abstract.** The paper gives a picture about the current state of teaching and learning information security related topics within the ESP course at technical universities in the Russian Federation and Republic of Belarus. The research was completed on an example Russian University of Transport, Moscow, and Belorussian State University of Transport, Gomel. The results of thematic analysis of the materials of the Cyber Security Body of Knowledge (CYBoK) and International Federation of Information Processing (IFIP) the relevant themes are determined. The analysis of the ESP textbook showed that the thematic coverage is less than 50% of relevant themes. Some recommendations on improving the educational process are given.

**Keywords:** information security, ESP course, university, textbook, CYBoK, IFIP.

Преподавание английского языка для специальных целей (ESP) студентам технических университетов, обучающихся по специальностям, связанным с информационными технологиями, осуществляется в рамках курса профессионально ориентированного иностранного языка. Идея об изучении иностранного языка в контексте будущей профессиональной деятельности была предложена и обоснована А.А.Вербицким [1], ряд российских ученых горячо поддержали эту идею, что нашло отражение в работах [4, 2] и других.

Большой вклад в методику преподавания английского языка как иностранного (EFL) в российских университетах в целом и английского языка для специальных целей (ESP) в частности внесли британские методисты [8]. В настоящее время российские преподаватели, как и преподаватели иностранных языков всего мира, стремятся адаптировать положения методики обучения иностранным языкам к новой реальности для достижения главной цели – формирования профессиональной иноязычной коммуникативной компетенции у студентов бакалавриата. При этом тематика учебного общения должна быть актуальной и соответствующей требованиям времени.

В данной статье представлено исследование такой актуальной для специальностей, связанных с информационными технологиями, тематики, как информационная безопасность. Оценено текущее состояние преподавания и изучения тем, связанных с информационной безопасностью, в рамках курса английского языка в техническом университете, намечены пути совершенствования обучения, поскольку информационная безопасность становится приоритетной областью в современном цифровом мире.

Российский университет транспорта и Белорусский государственный университет транспорта являются отраслевыми университетами. Их акционеры-учредители – Министерство транспорта Российской Федерации и Министерство транспорта Республики Беларусь. Направления подготовки в сфере информационных технологий (09.00.00 – Информатика и вычислительная техника, 10.00.00 – Информационная безопасность в Российском университете транспорта и 6-05-0611-01 Информационные системы и технологии в Белорусском государственном университете транспорта) связаны с транспортным сектором.

В формирование образовательных программ включены несколько заинтересованных сторон: учащиеся, преподаватели и эксперты, родители учащихся [7], образовательные учреждения, поставщики контента, поставщики образовательных технологий, органы по аккредитации и работодатели [10]. Мы же в своей статье хотим показать, что образованием в области информационной безопасности крайне заинтересованы также и международные организации.

Задача нашего исследования заключалась в том, чтобы проанализировать актуальную тематику в сфере информационной безопасности, предлагаемую международными организациями, и изучить учебники ESP для студентов технических вузов, ведущих подготовку специалистов в области информационных технологий, с точки зрения соответствия признанной на международном уровне тематике.

При рассмотрении идей и концепций информационной безопасности, которые можно увязать с изучением ESP в технических вузах, была рассмотрена информация сайта Свод знаний по кибербезопасности, текущая версия 1.1. – The Cyber Security Body of Knowledge (<https://cybok.org>) и Международной федерации по обработке информации – International Federation for Information Processing (<https://ifip.org/tc/?tc=tc11>).

Структура и содержание Свода знаний по кибербезопасности (CYBoK) версии 1.0. подробно описана в работе В.А.Сухомлина, Е.В.Зубаревой [5]. В их работе указывается, что в проекте CYBoK произведена систематизация знаний по кибербезопасности. В текущей версии 1.1. этот Свод содержит 21 компетенцию (Knowledge Areas), сгруппированные в пять категорий:

1. Человеческие, организационные и нормативные аспекты – **Human, Organisational & Regulatory Aspects**. В эту категорию включены такие компетенции, как: **Управление рисками и руководство, Законы и предписания, Человеческие факторы, Конфиденциальность и онлайн права**.

2. Атаки и защита – **Attacks and Defences**. Данная категория содержит компетенции: Вредоносные программы и атакующие технологии, Состязательное поведение, Операции по безопасности и управление инцидентами, Криминалистика.

3. Безопасность систем – **Systems Security**. Категория включает в себя компетенции: Криптография, Безопасность операционных систем и виртуализации, Безопасность

распределенных систем, Формальные методы безопасности, Аутентификация, авторизация и учетность.

4. Безопасность программного обеспечения и платформ – Software and Platform Security. Компетенции, которые входят в данную категорию, следующие: Безопасность программного обеспечения, Безопасность веб и мобильных приложений, Безопасный жизненный цикл программного обеспечения.

5. Безопасность инфраструктуры. Компетенции данной категории: Прикладная криптография, Сетевая безопасность, Безопасность аппаратного, Безопасность киберфизических систем, Безопасность физического уровня.

По мнению В.А.Сухомлина и Е.В.Зубаревой, Свод знаний СУВоК может быть использован в качестве справочника при разработке образовательных программ разного уровня, и такие разработки уже имеются [**Ошибка! Источник ссылки не найден.**]. По моему мнению, СУВоК может быть использован для выявления актуальной тематики и разработки заданий и упражнений, затрагивающих вопросы кибербезопасности, для включения в курс ESP для студентов технических вузов укрупненных групп специальностей 09.00.00 – Информатика и вычислительная техника и 10.00.00 – Информационная безопасность (Россия) и 6-05-0611-01 Информационные системы и технологии (Республика Беларусь).

Международная федерация по обработке информации (IFIP) была основана в 1960 году с целью создания и распространения знаний по ИКТ во всем мире, продвижения идей цифрового равенства, повышения цифровой грамотности населения и профессионализма специалистов, а также для обеспечения общения на международном уровне. В составе Международной федерации по обработке информации работают четырнадцать технических комитетов; вопросами безопасности и защиты данных в информационных системах обработки информации занимается технический комитет 11 (TC-11). В его составе 14 рабочих групп (WG):

WG 11.1: Information Security Management – Управление информационной безопасностью. Занимается как чисто управленческими вопросами, такими как разработка стратегии безопасности на высшем уровне управления, так и техническими вопросами, связанными с управлением безопасностью, аварийным восстановлением и непрерывностью бизнеса.

WG 11.2: Pervasive Systems Security – Безопасность систем общего доступа (всепроницающих систем). Типичными характеристиками всепроницающей системы являются узлы с ограниченными ресурсами, часто физически недоступные или не имеющие пользовательского интерфейса, для обеспечения безопасности которых требуются специфические технические решения.

WG 11.3: Data and Application Security and Privacy – Безопасность и конфиденциальность данных и приложений. Занимается вопросами продвижения и внедрения новых технических решений по защите и конфиденциальности данных и приложений.

WG 11.4: Network & Distributed Systems Security – Безопасность сетей и распределенных систем. Рассматривает вопросы безопасности внутренних информационных систем организации при взаимодействии с внешней информационной средой, а также защитой киберпространства (криптография, компьютерная безопасность, сетевая безопасность и обеспечение информационной безопасности).

WG 11.5: IT Assurance and Audit – Обеспечение безопасности информационных технологий и контроль. В ведении этой рабочей группы достоверность и целостность информации, в том числе, финансовой отчетности.

WG 11.6: Identity Management – Управление идентификацией пользователей (включая биометрию).

WG 11.7: Information Technology: Misuse and The Law – Правовые вопросы использования информационных технологий, сюда входят киберполитика, управление и законодательство в области кибербезопасности.

WG 11.8: Information Security Education – Образование в области информационной безопасности. Разработка учебных курсов и программ обучения в университетах и других образовательных учреждениях.

WG 11.9: Digital Forensics - Цифровая криминалистика (аппаратная и программная криминалистика хостов и сервисов, мобильных устройств, встраиваемых систем, реагирования на инциденты, киберпреступности и обеспечения кибер-правопорядка).

WG 11.10: Critical Infrastructure Protection – Защита критической инфраструктуры (SCADA, IoT и промышленные системы управления).

WG 11.11: Trust Management – Управление сертификатами безопасности, например, в электронной коммерции, при предоставлении электронных государственных и других услуг.

WG 11.12: Human Aspects of Information Security and Assurance – Человеческие аспекты в обеспечении информационной безопасности (включая социальную инженерию).

WG 11.13: Information Systems Security Research – Исследования в области систем защиты информации (совместно с рабочей группой WG 8.11)

WG 11.14: Secure Engineering – Инженерия безопасности (кибератака и проникновение тестирование, обратный инжиниринг и криптоанализ).

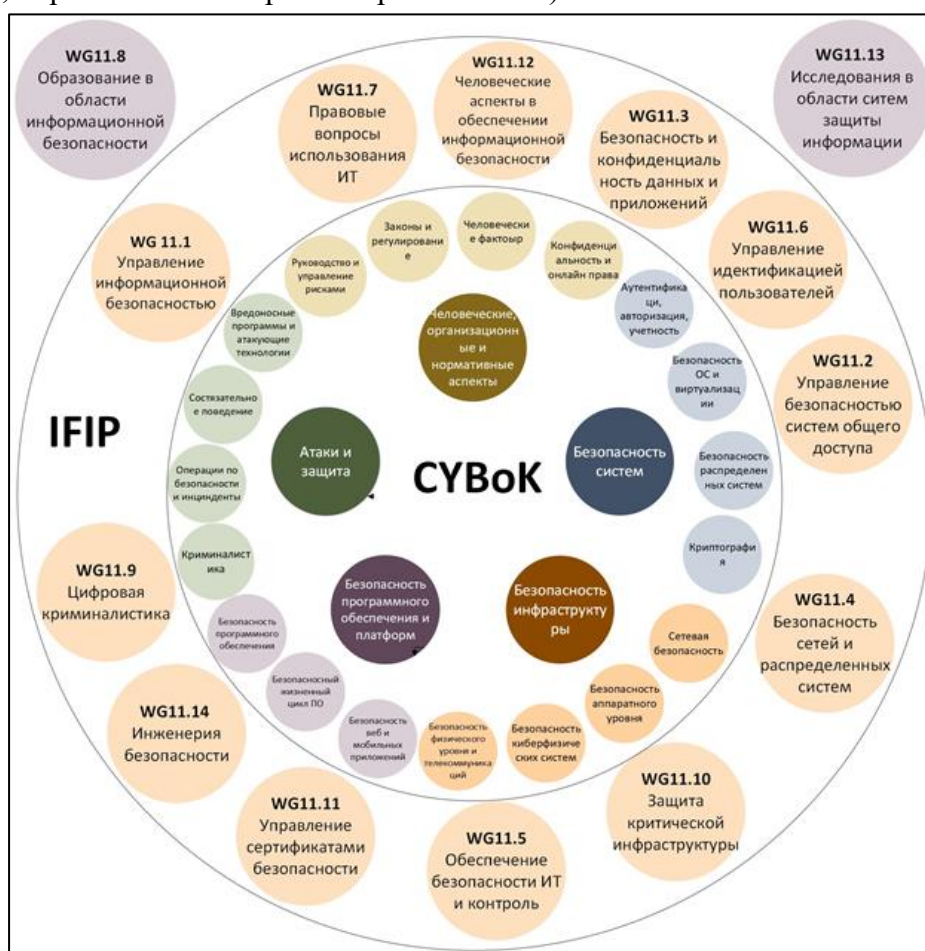


Рис. 1 - Сопоставление компетенций (Knowledge Areas) Свода знаний по кибербезопасности CYBoK и тематики Рабочих групп (WG) Международной федерации по обработке информации (IFIP)

На рисунке 1 во внутреннем круге представлены компетенции (Knowledge Areas) Свода знаний по кибербезопасности CYBoK, относящиеся к пяти категориям, размещенным в центре рисунка. Во внешнем круге представлена тематика Рабочих групп (WG) Международной федерации по обработке информации (IFIP). Можно заметить, что тематика, заявленная в Своде знаний CYBoK, практически полностью совпадает с тематикой работы IFIP. Однако

Международная федерация по обработке информации считает своей областью интересов публикацию научных исследований в области защиты информации и образование в области информационной безопасности.

Таким образом, на основе тематического анализа свода знаний СУВоК и тематики работы IFIP по первой части исследования можно сделать вывод, что вопросы информационной безопасности пронизывают практически все компьютерные науки, и в том или ином объеме должны изучаться студентами, обучающимися по специальностям укрупненных групп 09.00.00 – Информатика и вычислительная техника и 10.00.00 – Информационная безопасность (Россия) и 6-05-0611-01 Информационные системы и технологии (Республика Беларусь), в рамках всех учебных дисциплин.

На втором этапе исследования определено, каким образом вопросы информационной безопасности отражены в учебниках и учебных пособиях по английскому языку, используемых в технических вузах при обучении студентов компьютерных специальностей и направлений подготовки. Сегодня на рынке печатной продукции их действительно очень много. Мы подробно рассмотрели один из самых широко используемых в высшем образовании Российской Федерации и Республики Беларусь британских учебников профессионально-ориентированного английского языка (ESP) “Professional English in Use. For Computers and the Internet. ICT”, авторов Esteras S.R., Fabre E.M., издательство Cambridge University Press.

Анализ содержания учебника проведен путем сопоставления тематики Рабочих групп WG IFIP с тематикой текстов, а также заданий и упражнений 32 разделов данного учебника (Units), охватывающих различные аспекты использования информационных технологий. Результаты анализа представлены в Таблице 1.

Таблица 1. Аспекты информационной безопасности, нашедшие свое отражение в учебнике по английскому языку авторов Esteras S.R., Fabre E.M., издательство Cambridge University Press.

<b>Актуальная тематика в сфере информационной безопасности</b>	<b>Наличие текстов, заданий и упражнений по актуальной тематике</b>
Управление информационной безопасностью.	+
Безопасность систем общего доступа (всепроницающих систем).	+
Безопасность и конфиденциальность данных и приложений.	–
Безопасность сетей и распределенных систем.	+
Обеспечение безопасности информационных технологий и контроль.	–
Управление идентификацией пользователей	+
Правовые вопросы использования информационных технологий	–
Образование в области информационной безопасности	*ауд
Цифровая криминалистика	–
Защита критической инфраструктуры	–
Управление сертификатами безопасности – электронная коммерция и др.	–
Человеческие аспекты в обеспечении информационной безопасности	+
Исследования в области систем защиты информации	*ауд
Инженерия безопасности	+

Как видно из этой таблицы, почти 50% тематических аспектов информационной безопасности отражены в данном учебнике зарубежных авторов. Следует обратить внимание, что вопросы образования в области информационной безопасности, не вошедшие в учебник, непременно изучаются на занятиях в рамках темы «Моя будущая специальность». То же можно сказать и об исследованиях в области защиты информации. Высоко мотивированные студенты с хорошим уровнем английского языка имеют возможность принять участие и принимают его в научных конференциях разного уровня, проводимых на английском языке.

Итак, в ходе исследования была выявлена актуальная тематика, связанная с информационной безопасностью, и проанализирован один из популярных учебников английского языка для студентов, получающих образование в области информационных технологий. Результаты показали, что рассмотренный учебник затрагивает около 50% из актуальных тем информационной безопасности.

Тем не менее, большое количество преподавателей английского языка обладают передовым опытом в преподавании тем, связанных с информационной безопасностью, организуют проектную работу, конференции, ролевые игры, тематические исследования и семинары на английском языке. Необходимо, на наш взгляд, при изучении любой темы, связанной с информационными технологиями, затрагивать вопросы информационной безопасности, на том уровне, который соответствует знаниям и общей осведомленности студентов. Это могут быть вопросы или диалоги по ситуациям:

- при изучении темы «Мобильные устройства»: Как найти утерянный мобильный телефон? Как защитить мобильный телефон от несанкционированного доступа? Опасно ли расплачиваться за покупки мобильным телефоном? Могут ли за нами следить с помощью мобильных телефонов?

- при изучении темы «Операционные системы»: Нужна ли защита операционных систем? Какая операционная система лучше защищена от вирусов и других угроз?

- при изучении темы «Хранение информации»: Что безопаснее – хранить информацию в интернете, на флешке, на съемном диске или на оптическом диске? Какое устройство хранения надежнее?

- при изучении темы «Мультимедиа»: Каким образом можно защитить мультимедийные информационные продукты? Достаточно ли водяных знаков (watermarking) для защиты изображений? Как можно защитить видео на Youtube?

На продвинутом уровне можно предложить обсудить вопросы: Что такое социальная инженерия? Почему некоторые люди попадают на удочку мошенников? и другие.

Безусловно, идеи для интересных дискуссий собираются преподавателями по крупицам, их можно найти в опубликованных работах, в новых учебных материалах, например [3], и эта деятельность должна быть продолжена в соответствии с требованиями времени. Дисциплина «Иностранный язык» может внести весомый вклад в повышение осведомленности студентов транспортных университетов в области информационной безопасности.

### **Список литературы**

1. Вербицкий А.А. Новая образовательная парадигма и контекстное обучение /Монография. — М.: Исследовательский центр проблем качества подготовки специалистов, 1999.
2. Григоренко О.А. Контекстная модель профессионально направленного обучения: На материале иностранного языка в военном вузе//// Дисс.... канд. пед. наук / Москва, 2001.
3. Кузякин А. С. English for Information Technology 1: Pre-Intermediate and Intermediate. Учебное пособие. – М.: Белый ветер, 2022. – 236 с.
4. Маслова Ю.В. Содержание и формы иноязычной речевой деятельности студентов педвуза в контекстном обучении (на материале английского языка). // Дисс.... канд.

пед. наук / Липецкий государственный педагогический университет им. П.П. Семенова-Тян-Шанского. Липецк, 2000.

5. Сухомлин, В. А. Новый этап международной стандартизации ИТ-образования / В. А. Сухомлин, Е. В. Зубарева. – DOI 10.25559/SITITO.17.202103.697-723 // Современные информационные технологии и ИТ-образование. – 2021. – Т. 17, No 3. – С. 697-723.

6. Сухомлин, В. А. Создание профиля «Кибербезопасность и искусственный интеллект» для направления подготовки ФИИТ на основе куррикулумного подхода / В. А. Сухомлин. – DOI 10.25559/SITITO.17.202103.724-734 // Современные информационные технологии и ИТ-образование. – 2021. – Т. 17, No 3. – С. 724-734.

7. Chapleo, Ch. & Sims, Ch. Stakeholder analysis in higher education. Perspectives. 2010. 14. 12-20. 10.1080/13603100903458034.

8. Hutchinson T., Water A., English for Specific Purposes. Cambridge University Press. 1987.

9. Strevens P. ESP after twenty years: a reappraisal, In Tichoo M. (ed.) ESP: State of the Art. Singapore: SEAMEO Regional Language Centre. 1988.

10. Wagner, N., Hassanein, K., Head, M.. E-learning in higher education: A stakeholders' analysis. Proceedings of the International Conference on Information Technology Interfaces, ITI. 2006. 307 - 312. 10.1109/ITI.2006.1708497.