

СОВМЕСТНАЯ ПРОГРАММА ПОДГОТОВКИ МАГИСТРОВ ERASMUS +

***Красов Андрей Владимирович, Ушаков Игорь Александрович,
Штеренберг Станислав Игоревич***

Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург
e-mail: krasov@indox.ru, Ushakovia@gmail.com ,shterenbergsstanislaw@yandex.ru

Аннотация. С 2013 года Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича (далее – СПбГУТ) принимает участие в реализации совместной международной программы подготовки магистров по направлению 10.04.01 «Информационная безопасность» «Educating the next generation experts in Cyber Security: The new EU-recognized Master's program» (Магистерская программа нового поколения экспертов в информационной безопасности, признанная ЕС) (ENGENSEC).

В реализации программы принимают участие ведущие ВУЗы России, Германии, Швеции, Греции, Украины, Латвии, Польши. В ходе реализации программы был создан совместный блок дисциплин для всех Вузов участников, осуществлялась подготовка преподавателей, взаимные обмены студентов и преподавателей ВУЗов участников проекта. Данная программы дважды проходила мониторинг Европейской комиссии по образованию.

Исходя из опыта участия в данном проекте можно сделать вывод о том, что подобное взаимодействие ВУЗов разных стран и есть лучший критерий для проверки качества совместных международных программ.

Ключевые слова: ENGENSEC, магистерская программа, СПбГУТ, информационная безопасность, международная программа, сетевое обучение

Международное сотрудничество – одно из важнейших направлений деятельности университета. Реализация программы подготовки магистров ENGENSEC позволила организовать сетевую форму обучения студентов между СПбГУТ и Blekinge Institute of Technology (BTH), включающая в себе также не только обмен студентами, но и взаимный обмен преподавателями для чтения лекций. Подписано соглашение об академической мобильности для преподавателей и студентов на 2014-2021 гг. Начиная с 2015/16 учебного года студенты СПбГУТ выезжают обучаться на семестр в Швецию, со своими курсами в Blekinge Institute of Technology (далее – BTH) выезжают и преподаватели кафедры ЗСС, а в СПбГУТ приезжают преподаватели из Швеции. Обучение осуществляется по согласованным учебным планам, включающим в себя унифицированный блок дисциплин. Данный обмен позволяет оценить качество организации учебного процесса в обоих университетах и способствует повышению навыков и обмену знаниями между ВУЗами.

Дважды данный проект подвергался мониторингу Европейской комиссии по образованию, все разработанные дисциплины прошли международную апробацию и лицензирование, как в каждом из ВУЗов, так и промышленных партнеров.

Важной задачей проекта являлась разработка новых курсов по информационной безопасности [1,2]. Для реализации задачи были задействованы лучшие эксперты узкопрофессиональных областей из академической и промышленной среды [3,4].

Реализация данного проекта, в котором принимают участие ведущие вузы России, Швеции, Германии, Польши, Греции и Украины, предполагает создание новой

унифицированной для всех вузов партнеров программы подготовки магистров, основанной на лучшем опыте каждого из участников (рис. 1). Индустриальными партнерами программы выступают ведущие научно-исследовательские центры стран участников [5], такие как Бундескриминал (Германия), Вроцлавский университет (Вроцлав, Польша), Эгейский университет (Греция) и Латвийский университет (Рига, Латвия), СПИИРАН (Россия). Главным вузом в программе выступает ВТН (Карлскруна, Швеция).



Рисунок 1 – Область сотрудничества ENGENSEC.

Летом 2016 года на базе кафедры успешно прошла международная летняя школа по проекту ENGENSEC. В течение двух недель студенты из разных стран изучали курсы по информационной безопасности повышенного уровня сложности. В работе школы приняли участие студенты следующих вузов: Технологического института Блекинге (Карлскруна, Швеция), Вроцлавского Технического Университета (Вроцлав, Польша), Ярославского государственного университета имени П.Г. Демидова (Ярославль, Россия), Калининградского государственного технического университета (Калининград, Россия) и Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича (Санкт-Петербург, Россия) [6].

Курсы, предложенные студентам для изучения, были разработаны в рамках проекта ENGENSEC международными командами экспертов из академической и индустриальной среды. В рамках международной летней школы были представлены следующие дисциплины совместной программы подготовки магистров в области информационной безопасности ENGENSEC: «Защита облачных вычислений и телекоммуникаций», «Цифровые доказательства», «Веб-безопасность», «Тест на проникновение и этичный хакинг». Преподавателями школы выступили эксперты из Технологического института Блекинге (Карлскруна, Швеция), Федерального ведомства уголовной полиции Германии (Висбаден, Германия), Харьковского национального университета радиозлектроники (Харьков, Украина), Калининградского государственного технического университета (Калининград, Россия), Санкт-Петербургского института информатики и автоматизации (Санкт-Петербург, Россия), Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича (Санкт-Петербург, Россия) и учебного центра «Эшелон». (Москва, Россия). Также, курс «Тест на проникновение и этичный хакинг», представленный

Александром Дорофеевым из НПО Эшелон, г. Москва являлся заключительным в рамках международной Летней школы, проводившейся на базе СПбГУТ [6,7].

По поручению Европейской комиссии, Национальным офисом программы Erasmus+ (Темпус) в России был проведен мониторинг реализации проекта. Мониторинг – плановая проверка, некоторый аналог процедуры аккредитации [8].

В табл. 1 представлены вопросы, обсуждаемые в ходе мониторинга, которые разделяются на категории: значимость, результативность, эффективность, потенциал устойчивости. Мониторинг предполагает:

1. встречи с максимально большим количеством участников проекта с обязательным присутствием координатора проекта от СПбГУТ;
2. участие представителей университетов-партнеров (по возможности);
3. отдельные встречи с сотрудниками администрации проекта, преподавателями, занятыми в проекте и студентами;
4. встречу с ректором/ проректором университета (не более чем на 30 минут)
5. ознакомление с проектной документацией, списком участников промежуточными отчетами, историей проекта и т.д.

Таблица 1. Перечень вопросов и их конкретизация для обсуждений в ходе реализации мониторинга

Вопросы для обсуждения в ходе мониторинга			
Обзор задач и результатов проекта (для выяснения того, соблюдаются ли они или претерпели изменения, а также степени достижения результатов проекта)	Состояние реализации проекта на момент мониторинга (по log-frame), включая эффективность и качество реализации. Следует обратить особое внимание на мнение потребителей (студентов, обучающихся), а также различных категорий сотрудников проекта.	Воздействие (непосредственно связано с качеством) – степень распространения результатов на факультете/кафедре/учебном заведении и системе ВО в целом.	Устойчивость – жизнеспособность проекта после завершения финансирования
Значимость:	Результативность:	Эффективность:	Потенциал устойчивости:
-нужно ли было как-то изменять задачи для удовлетворения потребностей страны-партнера или учебного заведения страны партнера; -как реагировал проект на внешние изменения и как это отражено в структуре проекта (задачи, допущения и риски); -насколько остаются значимыми ожидаемые результаты и мероприятия, допущения и риски.	-соответствие мероприятий графику, менеджмент проекта; -достижение запланированных результатов в соответствии с графиком, верифицируемость показателей; -менеджмент и координация проекта: своевременность принятия решений и их адекватность для решения проблем и эффективной реализации поставленных задач; -гибкость проекта в части удовлетворения изменяющихся потребностей (адаптивность к внешним и внутренним факторам, модификация	-соответствие мероприятий/деятельности ожидаемым результатам; -вклад полученных результатов в достижение задач проекта; -участие заинтересованных сторон в управлении и реализации проекта; -возможность бенефициариев пользоваться достижениями проекта; -побочные результаты, запланированные и незапланированные, соответствующие задачам проекта; -адаптивность проекта к внешним изменениям.	-поддержка на политическом уровне; -вклад проекта в институциональное развитие; -содействие проекта решению социально-культурных вопросов и учет гендерных факторов; -экономическая, финансовая, социальная возможность использовать полученные результаты для учебных заведений страны-партнера; -степень участия в модернизации образования на уровне факультета/университета и роль проекта Темпус в процессах модернизации; степень обновления обучения и учебных программ и его влияние на повышение квалификации студентов; -способствует ли проект превращению университета в

	плана работы и бюджета).		«центр совершенства» в данной области или повышению престижа университета на национальном и международном уровне; -влияние проекта Темпус на процессы реформирования и модернизации высшего образования; его содействие реализации Болонского процесса; -влияние проекта на повышение процента трудоустройства выпускников и развитие взаимодействия университета с предприятиями.
--	--------------------------	--	--

К мониторингу подготавливается презентация о ходе реализации проекта и документальное подтверждение:

1. достигнутых результатов на момент мониторинга (разработанные курсы, модули, материалы и т.д.);
2. заинтересованности вуза в проекте;
3. всех рабочих встреч,
4. семинаров и их результатов (протоколы);
5. результативности стажировок и программы мобильности (отчеты);
6. распространения результатов и наработок проекта в вузе и за его пределами (перечень публикаций, презентаций, выступлений);
7. наличия эффективных механизмов управления проектом (распределение обязанностей, механизмы коммуникации и взаимодействия, протоколы рабочих встреч по управлению проектом, механизмы принятия решений);
8. наличия механизмов обеспечения качества проекта (критерии качества, механизмы мониторинга и внутренней и внешней оценки);
9. устойчивости результатов проекта;
10. значимости результатов для членов консорциума;
11. синергии данного проекта с проектами других доноров.

Мониторинг – это средство выявления ресурсов для оптимизации проектов программы Tempus в целом и каждого конкретного проекта, мониторинг которого осуществляется [8]. Мониторинг также помогает выявить проблемы и совместно осуществить пути их решения.

В задачи мониторинга входит получение наиболее полного представления о:

1. ходе реализации проектов;
2. промежуточных (или конечных) результатах;
3. возможностях распространения наработок проектов в университетском сообществе в России.

Мониторинг был успешно пройден кафедрой ЗСС в 2014 и 2017 году. Мониторинг осуществляла Муравьева А.А. – зам.директора Национального офиса Erasmus+ (Темпус) в РФ. Продолжительность мониторинга составляла 3 часа.

В настоящий момент СПбГУТ для продолжения обучения выбрали два будущих магистранта ВТН и в сентябре они приступят к программе обучения по направлению 10.04.01 «Информационная безопасность» в СПбГУТ. В течение года магистранты будут проходить обучение по общей программе подготовки на английском языке.

В ближайшей перспективе студенты направления 10.04.01 «Информационная безопасность», которые обучаются на кафедре Защищенных систем связи, также будут

иметь возможность получить **два диплома** о высшем образовании – один в СПбГУТ, другой диплом ЕС из ВТН.

Кафедра ЗСС уже перешла на реализацию подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность» (рис. 2) в рамках учебного плана, разработанного в ходе работы над проектом ENGENSEC [5].

ENGENSEC										Структура направления подготовки магистров										Tempus															
Educating the Next generation experts in Cyber Security										10.04.01 Информационная безопасность																									
Educatng the Next generation experts in Cyber Security: the new EU-recognized Master's program																																			
Подготовка ведётся в соответствии с профессиональным стандартом 06.032 "Специалист по безопасности компьютерных систем и сетей"																																			
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30						
Сертификация средств защиты информации			Технологии обеспечения информационной безопасности			Управление информационной безопасностью			Защищенные информационные системы			Технологии обеспечения информационной безопасности больших данных			Научно-исследовательская работа (НИР)																				
каф. ЗСС доц.Юркин Д.В. Зачет			каф. ЗСС ст. преп. Ушаков И.А. Экзамен			 каф. ЗСС доц. Сахаров Д.В. Экзамен			каф. ИУС доц. Мошак Н.Н. Зачет			каф. ЗСС доц. Чечулин А.А. Экзамен, КР			доц. Красов А.В. Зачет с оценкой																				
Защита облачных вычислений и телекоммуникаций						Тестирование на проникновение и этичный хакинг						Разработка защищенных приложений						НИР			Производственная практика														
Advanced Network & Cloud Security каф. ЗСС ст. преп. Ушаков И.А. Экзамен, КР						Pentest & Ethical Hacking каф. ЗСС ст. преп. Петрин Р.Б.  Экзамен						Secure Software Development каф. ЗСС доц. Красов А.В. Экзамен, КР						доц. Красов А.В. Зачет с оценкой			доц. Красов А.В. Зачет с оценкой														
Технологии защиты беспроводных сетей и мобильных приложений						Вредоносное программное обеспечение						Цифровая криминалистика						Научно-исследовательская работа (НИР)																	
Wireless & Mobile Security каф. ЗСС доц. Ковзур М.М., ст.преп. Кириллов Д.И. Экзамен, КР						Malware каф. ЗСС доц. Красов А.В. Экзамен, КР						Digital Forensic каф. ЗСС prof. Anders Carlsson, доц. Чечулин А.А. Дойникова Е.В.  Bundeskriminalamt Экзамен, КР						доц. Красов А.В. Зачет с оценкой																	
Производственная практика										Преддипломная практика										Итоговая аттестация															
доц.Красов А.В.										Красов А.В.										Кириллов Д.И.															

Рисунок 2 - Структура направления подготовки магистров

Проект ENGENSEC финансируется при поддержке Европейской Комиссии; EACEA, Tempus IV. Проект обратил внимание на проблемы развития информационного общества, направлен на кибербезопасность и конфиденциальность в электронном мире. В ходе осуществления проекта разрабатывается расширенный магистерский учебный план для обучения экспертов нового поколения, основанный на успешном опыте внедрения двойных дипломов среди студентов ЕС, европейской системе переводных зачетных единиц и обоюдном признании дипломов [6,7].

Начиная со второго семестра, студенты уже изучают дисциплины, разработанные в рамках работы над созданием магистерской программы нового поколения экспертов в области информационной безопасности, признанной ЕС (ENGENSEC) [4,5]. Это унифицированный блок, состоящий из 43-45 зачетных единиц, разрабатываемый всеми шестью странами-участниками.

На втором семестре читаются дисциплины:

1. Advanced Network&Cloud Security (Защита облачных вычислений и телекоммуникаций).
2. Wireless&Mobile Security (Технологии защиты беспроводных сетей и мобильных приложений).
3. Secure software development (Разработка защищенных приложений на java).
4. Malware (Вредоносное ПО).

5. Pentest and ethical hacking (Тест на проникновение и этический хакинг).

6. Digital forensic (Основы стеганографии)

Заключительный семестр в учебном плане посвящен разработке и защите диссертации на соискание ученой степени магистра в области информационной безопасности. Работа над темой диссертации начинается с первого семестра обучения. Магистры обязательно делают доклады на секции кафедры на научно-технической конференции нашего университета, публикуют статьи по результатам своих исследований.

Такие совместные программы - лучший способ оценки качества, новый путь совершенствования учебного процесса. Учета опыта всех партнеров ВУЗов из разных стран. В результате реализации проекта ENGENSEC, магистранты получили доступ к новым учебным материалам, повысили квалификацию преподаватели, укрепилась лабораторная база за счет приобретения нового оборудования, открытие магистерской подготовки экспертов информационной безопасности по программе нового поколения содействует развитию международного сотрудничества и мобильности студентов.

Особенностью данной образовательной программы является отбор ее Еврокомиссией для участия в программе Темпус. Это участие предполагает не только совместную разработку учебно-методических материалов, но и возможность получения студентами **двух дипломов** – нашего университета и одного из вузов-партнеров.

В качестве примера, в конце января 2016 года студенты кафедры ЗСС поехали в Технологический институт Блекинге (Blekinge Tekniska Högskola, ВТН) как первые студенты СПбГУТ, принявшие участие в магистерской программе международного обучения экспертов в информационной безопасности ENGENSEC. Вот их отзыв об участии в программе:

«Хочется сказать, что эта поездка дала нам возможность ощутить на себе то, как живут, учатся и работают шведы, и взглянуть на европейскую систему образования. Это был довольно интересный опыт, и на наш взгляд, если у вас есть возможность поехать в ВТН, то вы должны ей обязательно воспользоваться. Большое спасибо кафедре ЗСС, за то, что они дали нам такую возможность и за активное содействие и помощь».

Список литературы

1. Ушаков И.А. Подготовка специалистов в области информационной безопасности в СПбГУТ, / Ушаков И.А., Красов А.В. // Журнал "Инновации", 2013, №7. С. 92-97
2. Красов А.В. Реализация совместных образовательных программ в области информационной безопасности с республикой Вьетнам. / Красов А.В., Ушаков И.А., Левин М.В. // Управление качеством в образовательных и научных организациях. Сборник статей. СПб. 2013
3. Красов А.В. Состояние и перспективы разработки учебно-методического комплекса по дисциплине "криптографические методы и средства обеспечения информационной безопасности инфокоммуникаций" в соответствии с ГОС ВПО третьего поколения. / Красов А.В., Коржик В.И., Яковлев В. А. // "Актуальные проблемы инфокоммуникаций в науке и образовании" II-я международная научно-техническая и научно-методическая конференция: Сборник научных статей. СПб: СПбГУТ, 2013 с. 832-834.
4. Красов А.В. Роль Научно-образовательного центра "Лаборатория Cisco" в подготовке специалистов в области инфокоммуникаций., / Красов А.В., Ушаков И.А. //XII Международная научно-практическая конференция вузов и факультетов инфокоммуникаций. Труды конференции. М.: МТУСИ, 2012, с. 82-84.

5. Красов А.В. Магистерская программа нового поколения экспертов в информационной безопасности, признанная ес (engensec) / Красов А.В., Ушаков И.А., Штеренберг С.И. // Современное образование: содержание, технологии, качество. 2015. № 1. С. 79-81.
6. Кафедра Защищенных систем связи: сайт. – URL: <http://zss.sut.ru> (дата обращения: 28.10.2019). – Текст: электронный.
7. Educating the Next generation experts in Cyber Security: сайт. – URL: <http://engensec.eu/> (дата обращения: 28.10.2019). – Текст: электронный.
8. Мониторинг проектов. сайт. – URL: <http://www.tempus-russia.ru/monitor.htm> (дата обращения: 28.10.2019). – Текст: электронный.

JOINT MASTER PROGRAM ERASMUS +

Krasov A.V., Ushakov I.A., Shterenberg S.I.

The Bonch-Bruевич Saint-Petersburg
State University of Telecommunications, Saint-Petersburg
e-mail: krasov@indox.ru, Ushakovia@gmail.com ,shterenberg.stanislaw@yandex.ru

Abstract. *Since 2013, St. Petersburg State University of Telecommunications named after prof. M.A.Bonch-Bruевич (hereinafter - SPbGUT) takes part in the implementation of a joint international program for the preparation of masters in the direction of 10.04.01 "Information Security" "Educating the next generation experts in Cyber Security: The new EU-recognized Master's program" (Master's EU New Generation of Information Security Experts Program (ENGENSEC).*

The leading universities of Russia and Germany take part in the implementation of the program. Sweden, Greece. Ukraine, Latvia, Poland. During the implementation of the program, a joint unit of disciplines was created for all universities of participants, training of teachers, mutual exchanges of students and teachers of universities of project participants were carried out. This program has been monitored twice by the European Commission on Education.

Based on the experience of participation in this project, we can conclude that such interaction between universities of different countries is the best criterion for checking the quality of joint international programs.

Keywords: *ENGENSEC, master's program, SPbSUT, information security, international program, network education*