

РЕАЛИЗАЦИЯ ДИСЦИПЛИН В ОБЛАСТИ СЕТЕВОЙ БЕЗОПАСНОСТИ СОВМЕСТНОЙ ПРОГРАММЫ ПОДГОТОВКИ МАГИСТРОВ В ДИСТАНЦИОННОМ РЕЖИМЕ

Красов А.В., Штеренберг С.И.

Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича

e-mail: krasov@inbox.ru; shterenberg.stanislaw@yandex.ru

Аннотация. В статье рассмотрен опыт использования дистанционных образовательных технологий в особых условиях опасности распространения новой коронавирусной инфекции. Особенностью кафедры ЗСС является то, что большинство наших курсов относятся к так называемому «тяжелому» контенту, требующему больших вычислительных ресурсов, а при удаленном подключении студентов - больших мощностей канала связи и постоянного наличия УВП для перенастройки и обслуживания оборудования в очном режиме на кафедре.
Ключевые слова: ENGENSEC, магистерская программа, СПбГУТ, информационная безопасность, международная программа, дистанционное обучение

Структура образовательных программ кафедры Защищенных систем связи

Кафедра ЗСС является выпускающей по 3-м направлениям подготовки бакалавров (рисунок 1) и инженеров:

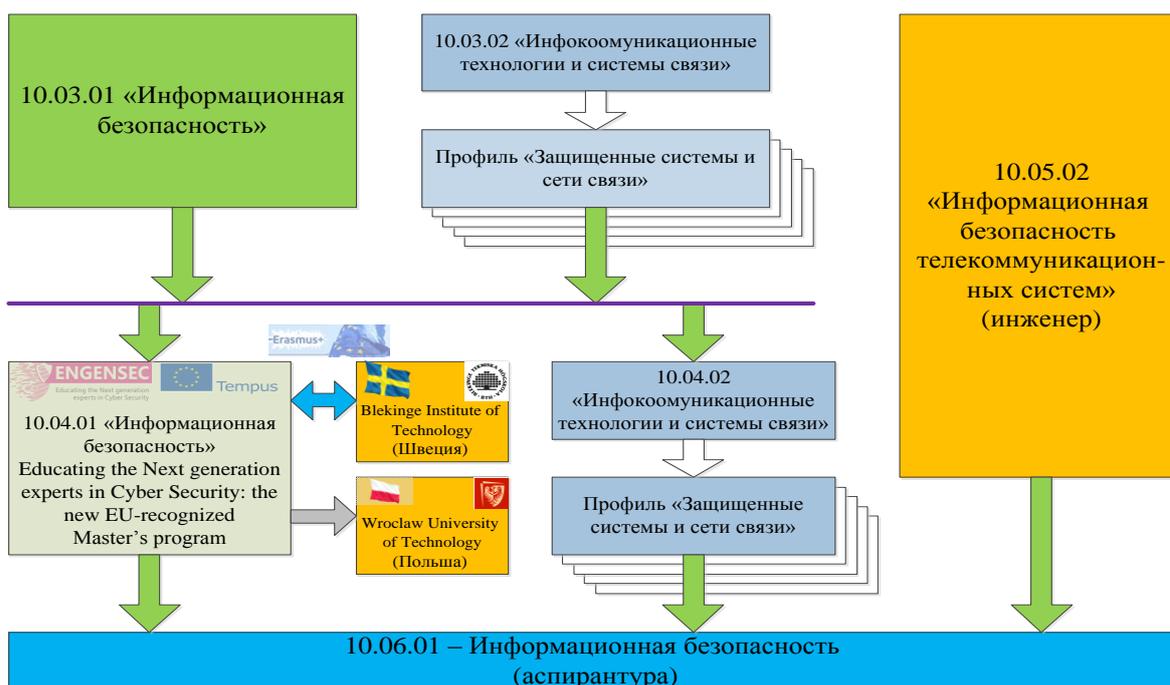


Рисунок 1 - Структура образовательных программ кафедры ЗСС

- 10.03.01 «Информационная безопасность» (4-5 групп);
- 11.03.02 «Инфокоммуникационные технологии и системы связи» по профилю «Защищенные системы и сети связи» (2 группы);
- 10.05.02 «Информационная безопасность телекоммуникационных систем», специализация №12 «Безопасность телекоммуникационных систем информационного взаимодействия».

На следующем уровне подготовки кафедра реализует программы подготовки магистров:

- 10.04.01 «Информационная безопасность» - магистерская программа, признаваемая Европейским Союзом [1,2] (Educating the Next generation experts in Cyber Security: the new EU-recognized Master's programm ENGENSEC (2 группы);
- 11.04.02 «Инфокоммуникационные технологии и системы связи» по профилю «Защищенные системы и сети связи» [3,4] (1 группа).

По программам подготовки кадров высшей квалификации (аспирантура) кафедра осуществляет подготовку по направлению подготовки научных кадров:

- 10.06.01 Информационная безопасность, направленность 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Ежегодно кафедра набирает более 350 студентов по всем видам образования. Всего на кафедре обучается почти 1000 студентов.

В рамках УГС 10.00.00 Информационная безопасность в силу специфики данного направления подготовки реализация заочной формы обучения не предусмотрена, а использование дистанционных технологий ограничено. Кафедра более 20 лет ведет только очное обучение студентов.

Ситуация с новой коронавирусной инфекцией поставила кафедру в тяжёлые и нетипичные условия. Первый опыт мы получили в прошлом семестре – начиная с 8 недели учебный процесс был переведен на дистанционный режим. К этому времени учебный процесс бакалавров 4-го курса (последнего) был уже завершён (он короче), и мы завершили значительную часть самых сложных лабораторных работ. Понимая, к чему идет дело, мы форсировали темп выполнения лабораторных работ по всем нашим дисциплинам, оставив на конец весеннего семестра сдачи отчетов.

Текущий осенний семестр начался нестабильно: группы или лекционные потоки, в которых были заболевшие студенты, переходили на 2-х недельный карантин. Но за счет высокой дисциплины наших студентов число заболевших было невелико, поэтому большинство занятий пошло в штатном режиме. С 15 ноября кафедра ЗСС вновь была полностью переведена на дистанционный режим. В целом, выявились следующие проблемы в связи с особым режимом работы:

- студенты из РФ сумели выехать для начала штатного семестра в ВТН (Швеция);
- студенты из Швеции, Замбии, Армении не смогли приехать к нам;
- начало учебного года – одновременное проведение и очных, и дистанционных занятий;
- двойной контроль как нашего вуза, так и вузов-партнеров.

Возможности проведения занятий в системе Discord, сравнение с ZOOM и Skype

В связи с окончанием 5 апреля каникул возобновилось проведение образовательного процесса согласно приказу ректора университета от 17.03.2020 г. №154 «Об организации образовательной деятельности в условиях предупреждения распространения новой коронавирусной инфекции на территории Российской Федерации» [6,7]. Учебный процесс осуществляется в электронной информационной образовательной среде (ЭИОС) университета с использованием различных образовательных технологий, в том числе с применением электронного обучения и дистанционных технологий в системе Discord.

В Discord [10] можно использовать голосовой чат, текстовый чат, видеосвязь и, с недавнего времени, демонстрацию экрана для участников сервера. Другими словами, преподаватель может общаться со студентами следующим образом: преподаватель рассказывает – студенты слушают, преподаватель спрашивает кого-то конкретно - студент отвечает, можно показать алгоритм решения или выполнения задания при помощи режима видео, можно, используя демонстрацию экрана, показать студентам какие-то таблицы, иллюстрации или презентации. Еще можно отправлять файлы (картинки, документы) прямо в текстовом чате. Они, соответственно, выполнив задание, могут отправить обратно.

Спрос на программы «Zoom» и «Skype» за последние дни вырос в разы. Однако у подобных сервисов встречается ряд недостатков, которыми Discord не обладает:

- групповые конференции доступны только 40 минут, дальше нужно активировать платную версию;
- в начале работы с программой необходимо немного в ней разобраться и вникнуть в принцип работы; особенно, если вы преподаете в группах;
- в программе есть уязвимости, которые могут приводить к утечкам персональных данных пользователей;
- Skype – очень «тяжелая» программа для старых ноутбуков; она тянет много ресурсов, подвисает сама и тормозит работу других программ;
- тяжело транслирует Skype видео и звук, выжимая из компьютера много ресурсов;
- можно вывести только демонстрацию своего экрана, но не отдельных приложений.

У кафедры был доступ CiscoWebex – лучшей профессиональной платформы для организации удаленного учебного процесса, предоставленной бесплатно всем вузам-участникам партнёрских сетевых академий, в том числе и нам на время пандемии. Но данное решение требовало согласовывать расписание занятий с менеджментом, расположенным на территории США, что было нежелательно для программ в области информационной безопасности.

Но, несмотря на хороший функционал, у «Zoom» большие проблемы в обеспечении конфиденциальности пользователей. Так приложение не поддерживает сквозное шифрование данных и имеет другие серьёзные бреши в системе безопасности, которые возникали как раз по причине добавления некоторых функций [9]. Функция AttendeeAttentionTracking (отслеживания внимания слушателей) позволяет вычислять тех, кто отвлекается от беседы на посторонние дела. Очевидно, что это кажется полезным руководителям компаний и ведущим учебных занятий, однако минусы этой функции значительно серьёзнее, поскольку она использует трекеры слежения (скрипты, осуществляющие удалённую слежку за всеми участниками), которые позволяют программе «обходить параметры безопасности в браузере и вести несогласованную слежку за пользователем и его действиями посредством веб-камеры», к чему неоднократно возникали вопросы со стороны специалистов по защите персональных данных. Выяснилось, что Zoom также преобразует в ссылки UNC-пути, то есть пути к файлам в Windows. Используя такие ссылки, по которым размещены изображения, аудиозаписи и другие медиафайлы, хакеру не составит никакого труда взломать хэши и получить доступ к учётным данным пользователей Zoom [9]. В компании знают об этой уязвимости, однако пока никаких исправлений кода приложения не последовало.

С апреля 2020 года в связи с новой короновирусной инфекцией кафедра ЗСС вынуждено перешла на ДОТ. Для проведения занятий была использована бесплатная программа Discord, которая создавалась для геймеров для обмена текстовыми и голосовыми сообщениями – по сути как интернет-телефон. Все важные и не очень функции в Discord бесплатны [10]. Программа позволяет организовать занятия с аудиторией до 100 студентов. Discord имеет следующие преимущества:

- хорошее качество звука и видео;
- отличная оптимизация программы – очень экономное использование ресурсов компьютера;
- понятный интерфейс, современный дизайн;
- возможность создания серверов (аналог групп в скайпе) с функцией разделения на подгруппы – чаты и присвоения участникам различных ролей;
- безопасность – в режиме стримера Discord блокирует все ваши данные от других пользователей;
- возможность добавления в ваши серверы ботов для развлечения и/или информирования посетителей.

Студенты при этом видят только демонстрацию экрана преподавателя в Discord. Преподаватели могут общаться со студентами, как будто они в аудитории. И посторонних в свой виртуальный класс преподаватель может не пускать. Discord – мессенджер с поддержкой VoIP и видеоконференций, изначально ориентированный на пользователей компьютерных игр [10]. Настольное клиентское приложение реализовано для Windows (работает на Windows 7 и новее), macOS и Linux, мобильное приложение — для Android, iOS, а также существует веб-клиент. Единая кодовая база для настольных, веб- и мобильных клиентов обеспечивается благодаря использованию фреймворка Electron. Серверы мессенджера размещены в 11 центрах обработки данных в разных частях мира. В этом мессенджере присутствуют продвинутое алгоритмы шифрования, которые позволяют сделать общение более безопасным. Есть встроенная защита от DDOS атак и вредоносного программного обеспечения. Также можно настроить двухфакторную аутентификацию. Если данная опция включена, то вход в аккаунт пользователя возможен только при подтверждении с помощью мобильного телефона.

О проекте Engensec

В качестве примера был выбран курс Защита облачных вычислений и телекоммуникаций из программы подготовки магистров 10.04.01 Информационная безопасность (рис. 2). Курс имеет следующий тематики:

- SDN – программно-конфигурируемые сети. Протокол OpenStack.
- NFV – Network Function Virtualization (виртуализация сетевых функций).
- безопасность SDN.
- Введение в облачные технологии, безопасность в облаке (Cloud Security: Confidentiality, Integrity, Accountability).

Экзамен проводится либо в формате онлайн, либо - статьи по теме дисциплины (бесплатный журнал – «Молодежная научная школа кафедры ЗСС»).

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	
<div style="display: flex; justify-content: space-between; align-items: center;"> <div style="text-align: center;"> <p>Структура направления подготовки магистров 10.04.01 Информационная безопасность</p> <p>Tempus</p> <p>Educating the Next generation experts in Cyber Security: the new EU-recognized Master's program</p> <p>Подготовка ведётся в соответствии с профессиональным стандартом 06.032 "Специалист по безопасности компьютерных систем и сетей"</p> </div> </div>																																																											
Сертификация средств защиты информации каф. ЗСС доц. Юркин Д.В. Зачет					Технологии обеспечения информационной безопасности каф. ЗСС ст. преп. Ушаков И.А. Экзамен					Управление информационной безопасностью каф. ЗСС доц. Сахаров Д.В. Экзамен					Защищенные информационные системы каф. ИУС доц. Мошак Н.Н. Зачет					Технологии обеспечения информационной безопасности больших данных каф. ЗСС доц. Чечулин А.А. Экзамен, КР					Научно-исследовательская работа (НИР) доц. Красов А.В. Зачет с оценкой																																		
Защита облачных вычислений и телекоммуникаций Advanced Network & Cloud Security каф. ЗСС ст. преп. Ушаков И.А. Экзамен, КР										Тестирование на проникновение и этический хакинг Pentest & Ethical Hacking каф. ЗСС ст. преп. Петров Р.В. Экзамен										Разработка защищенных приложений Secure Software Development каф. ЗСС доц. Красов А.В. Экзамен, КР										НИР доц. Красов А.В. Зачет с оценкой					Производственная практика доц. Красов А.В. Зачет с оценкой																								
Технологии защиты беспроводных сетей и мобильных приложений Wireless & Mobile Security каф. ЗСС доц. Ковалев М.М. ст. преп. Кириллов Д.И. Экзамен, КР										Вредоносное программное обеспечение Malware каф. ЗСС доц. Красов А.В. Экзамен, КР										Цифровая криминалистика Digital Forensic каф. ЗСС prof. Anders Carlsson, доц. Чечулин А.А., Добининова Е.В. Bundeskriminalamt Экзамен, КР										Научно-исследовательская работа (НИР) доц. Красов А.В. Зачет с оценкой																													
Производственная практика доц. Красов А.В.										Преддипломная практика Красов А.В.										Итоговая аттестация Иванов Д.И.																																							

Рисунок 2 - Структура направления подготовки магистров

Реализация проекта Engensec, 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. 3). 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). Головным вузом в программе выступает ВТН (Карлскруна, Швеция).

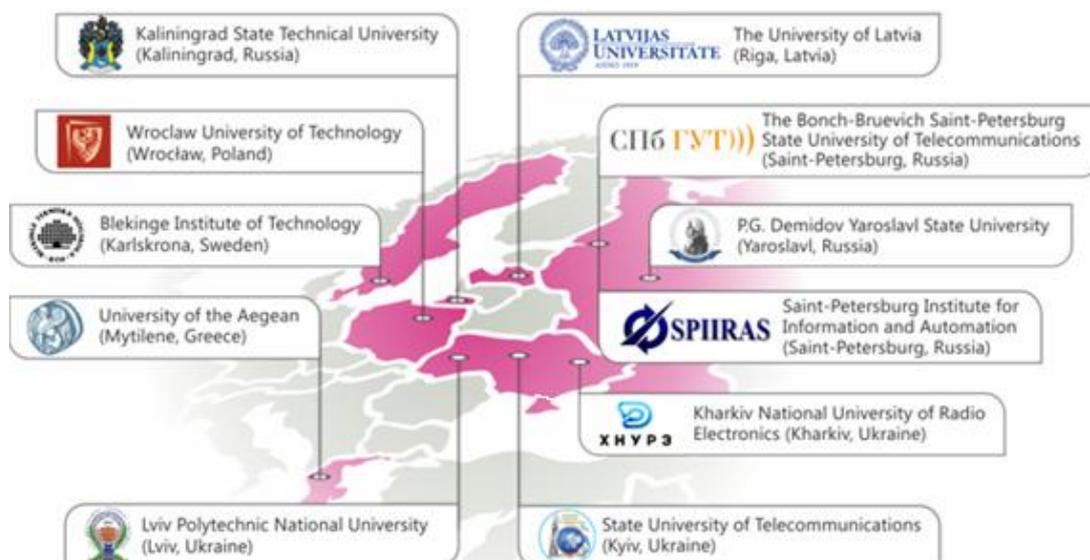


Рисунок 3 - Область сотрудничества ENGENSEC

Курсы, предложенные студентам для изучения, были разработаны в рамках проекта ENGENSEC международными командами экспертов из академической и индустриальной среды [7]. В рамках ДОТ 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 радиоэлектроники (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) [6,7].

Кафедра активно внедряет [6] разработанные в ходе проекта учебные курсы в образовательный процесс, используя переданное оборудование в рамках проекта «Erasmus+» (рис. 4). Прежде всего, комплекс RESELA – это не только серверное оборудование, но и программное обеспечение, которое позволяет организовывать учебный процесс на основе разработанных международными группами преподавателей комплексов лабораторных работ по унифицированным дисциплинам совместной программы подготовки магистров.



Наше оборудование (Грант [Россвязи](#));
Комплекс RESELA (Проект [Engensec](#), [Темпус](#))



Рисунок 4 - Удаленный доступ к оборудованию (состав оборудования)

Кафедре ЗСС удалось задействовать лабораторные стенды dCloud и создать ряд виртуальных лабораторных работ. dCloud – виртуальный комплекс компании Cisco (рис. 5), предоставляющий ресурсы дата-центров для проведения лабораторных работ. Имеет возможность создания нескольких сессий и их контроля. Лабораторные работы проводятся по самым передовым технологиям, включая SDN Cisco ACI, CiscoFirePower межсетевые экраны и многие другие.

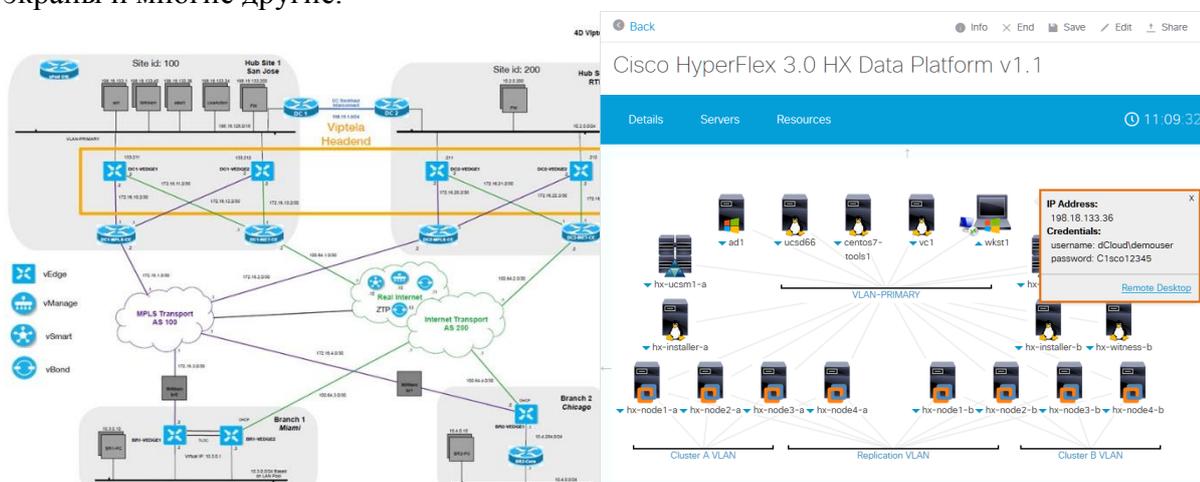


Рисунок 5 - dCloud виртуальные лабораторные работы (внешний интерфейс)

Выводы

В предыдущей статье [8] мы писали, что летние школы, международный обмен студентами и преподавателями – лучший инструмент проверки качества образования как у нас, так и у наших партнеров.

Наши студенты успели выехать на учебу в Швецию в сентябре [2,6]. Магистры из зарубежных стран не смогли приехать в Россию, они занимались дистанционно, и с 1 сентября мы транслировали им наши занятия, с 15 сентября все наши магистры, в том числе и из зарубежных стран, находятся на дистанционном режиме. Но эти занятия посещают не только те несколько студентов, которые должны были поехать на учебу в Россию, но и их друзья, преподаватели. И так как в рамках нашего совместного проекта EGENSEC этот блок дисциплин унифицирован и студенты могут перезачесть эти дисциплины, изученные в вузах-партнерах, студенты в большем количестве могут сравнивать организацию учебного процесса в разных странах. Наше образование стало почти открытым (среди вузов-партнеров): читая лекцию по данной магистратской программе, не знаешь, кто еще тебя слушает.

Раньше можно было подготовиться к выездным гостевым лекциям, натаскивать студентов на время приезда гостевого преподавателя, обеспечивать хорошее сопровождение тех нескольких студентов-иностранцев, которые приехали к нам. Теперь все стало сложнее, работать стало намного труднее, нагрузка на преподавателя резко возросла. Да, кто-то не тянет, а для кого-то открываются новые возможности.

Для магистрантов опыт использования новых технологий, включая удаленные стенды, показал лучшую посещаемость занятий за счет удобного формата проверки работ, подключения в любое время (даже вне официальных аудиторных часов). Для бакалавров удаленный формат обучения – скорее отрицательный опыт, т.к. студенты, в особенности обучающиеся на первых двух курсах, не отвыкли от очного формата обучения в школе – им требуется больший контроль за выполнением заданий.

Расширение контингента иностранных студентов за счет проведения интересных лабораторных работ, проводимых в удаленном формате, обеспечивает и их коллегам возможность подключения к виртуальным стендам. Это способствует продвижению лучших образовательных программ России, особенно в форме программ двух дипломов.

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.: МГУСИ, 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. Красов А.В., Совместная программа подготовки магистров ERASMUS + / Красов А.В., Ушаков И.А., Штеренберг С.И. // В сборнике: Новые технологии оценки качества образования. Сборник материалов XV Форума Гильдии экспертов в сфере профессионального образования. Под общей редакцией Г.Н. Мотовой. 2019. С. 156-162.
9. Zoom — банальная халатность или целенаправленный шпионаж?: сайт. – URL: <https://habr.com/ru/post/496812/> (Дата обращения: 18.12.2020). – Текст электронный
10. Discord как корпоративный мессенджер и не только: сайт. – URL: <https://habr.com/ru/post/495336/> Дата обращения: 18.12.2020). – Текст электронный

IMPLEMENTATION OF DISCIPLINES IN THE FIELD OF NETWORK SECURITY OF THE JOINT MASTER TRAINING PROGRAM IN REMOTE MODE

Krasov A.V., Shterenberg S.I.

Saint Petersburg State University of Telecommunications
them. prof. M. A. Bonch-Bruevich
e-mail: krasov@inbox.ru; shterenberg.stanislaw@yandex.ru

Abstract. *The article discusses the experience of using distance education technologies in special conditions of the danger of the spread of a new coronavirus infection. A special feature of the ZSS department is that most of our courses relate to the so-called "heavy" content that requires large computing resources, and with remote connection of students, large communication channel capacities and the constant availability of a UVP for reconfiguring and maintaining equipment in full-time mode at the department.*

Keywords: *ENGENSEC, master's program, SPbSUT, information security, international program, distance learning.*