ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

АРХАНГЕЛЬСКИЙ КОЛЛЕДЖ ТЕЛЕКОММУНИКАЦИЙ
ИМ. Б.Л. РОЗИНГА (ФИЛИАЛ) СПбГУТ
(АКТ (ф) СПбГУТ)

СОГЛАСОВАНО
Зам. директора по учебной работе
_____Н.В. Калинина
«14» ____09_____ 2020 г.

УТВЕРЖДАЮ
Директор АКТ (ф) СПбГУТ
_____А.П. Топанов
«22» _____09_____ 2020 г.

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ»

Архангельск 2020

Составитель:

А.А. Зубарев, преподаватель высшей квалификационной категории АКТ (ф) СПбГУТ.

Программа рассмотрена и одобрена цикловой комиссией Информационной безопасности инфокоммуникационных систем

Протокол № 1 от 24 сентября 2020г.

Председатель_____ А.А. Зубарев

СОДЕРЖАНИЕ

1 ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ «АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ»

1.1 Пояснительная записка

В условиях формирования инновационной экономики к системе профессионального образования предъявляют такие требования, как постоянное обновление технологий, ускоренное освоение инноваций, быстрая адаптация к запросам и требованиям. В этой связи активно внедряются стандарты WorldSkills в образовательный процесс.

Настоящая программа предназначена для повышения квалификации слушателей в области реализация образовательным программ с применением стандартов WorldSkills по направлению анализ защищенности информационных систем (которое является составляющей частью компетенции WorldSkills «Кибер-безопасность»).

Нормативно-правовой основой для разработки программы являются:

– Федеральный закон №273-ФЗ от 29 декабря 2012 г. «Об образовании в Российской Федерации»;

– Приказ Минобрнауки России от 01.07.2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

– Приказ Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 № 598н Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей»

– Методические рекомендации по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов (утверждены Министром образования и науки Российской Федерации 22.01.2015 г. № ДЛ-1/05вн).

1.2 Целевая аудитория

Программа предназначена для слушателей ведущих свою деятельность в области информационной безопасности (имеющих высшее или среднее профессиональное образование), а также преподавателей учебных дисциплин и МДК общепрофессиональных и профессиональных циклов, мастеров производственного обучения, учителей информатики образовательных организаций.

1.3 Цель программы и планируемые результаты обучения

Целью реализации программы является совершенствование профессиональной компетенции сотрудников организации в части сопровождение системы защиты информации в ходе её эксплуатации, проведение аттестации объектов вычислительной техники на соответствие

требованиям по защите информации, проведение аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации, а также педагогических работников системы профессионального образования, учителей информатики в области реализации образовательных программ.

В результате успешного освоения программы слушатель должен

уметь:

– восстановление работоспособности программно-аппаратных средств защиты информации в операционных системах согласно технической документации;

– выполнять проверку корректности работы программно-аппаратных средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

– настраивать компоненты подсистем защиты информации операционных систем;

– управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей.

знать:

– архитектуру и пользовательские интерфейсы операционных систем;

– порядок обеспечения безопасности информации при эксплуатации операционных систем;

– источники угроз информационной безопасности и меры по их предотвращению;

– сущность и содержание понятия информационной безопасности, характеристики ее составляющих;

– типовые средства защиты информации в операционных системах.

1.4 Нормативный срок освоения программы повышения квалификации

Нормативный срок освоения программы повышения квалификации составляет 30 часов, в том числе дистанционно – 4 часов.

1.5 Порядок аттестации слушателей

Текущий контроль знаний проводится по результатам выполнения практических работ.

Итоговая аттестация

Повышение квалификации завершается итоговой аттестацией, которая проходит в форме сдачи дифференцированного зачёта.

По завершении обучения слушателям выдается удостоверение о повышении квалификации.

2 СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

2.1 КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Календарный учебный график формируется непосредственно при реализации программы повышения квалификации «Анализ защищенности информационных систем». Календарный учебный график представлен в форме расписания занятий при наборе группы на обучение.

2.2 УЧЕБНЫЙ ПЛАН ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ «АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ»

№ п/п	Наименование разделов, модулей	Трудоемкость, ч.	Всего, ч.	в том числе					Самостоятельная работа, ч.	Форма аттестации
				Аудиторные занятия, ч.			Занятия с использованием ДОТ, ч			
				лекции	лабораторные занятия	практические занятия	лекции	практические занятия		
1	**Модуль 1 Основы работы с операционными системами**	**12**	**6**	0	0	4	0	2	**6**	Практическая работа №1-3 Самостоятельная работа №1-3
2	**Модуль 2 Инструменты анализа уязвимостей**	**10**	**8**	0	0	6	0	2	**2**	Практическая работа №4-7 Самостоятельная работа №4
3	**Модуль 3 Механизмы защиты**	**8**	**6**	0	0	6	0	0	**2**	Практическая работа №8-10 Самостоятельная работа №5
	Итого:	**30**	**20**	0	0	16	0	4	**10**	**Дифференцированный зачёт**

2.3 УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ «АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ»

№ п/п	Наименование разделов, модулей	Всего часов, ч.	Из них						Форма аттестации
			Аудиторные занятия, ч.			Занятия с использованием ДОТ, ч		Самостоятельная работа, ч.	
			лекции	лабораторные занятия	практические занятия	лекции	практические занятия		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
1	**Модуль 1 Основы работы с операционными системами**	**12**	**0**	**0**	**4**	**0**	**2**	**6**	Практические работы №№1-3 Самостоятельная работа №№1-3
1.1	**Практическая работа № 1** Установка и развёртка сетевой инфраструктуры для выполнения работ	2	0	0	2	0	0	0	
1.2	**Практическая работа № 2** Настройка компонентов операционных систем.	2	0	0	2	0	0	0	
1.3	**Практическая работа № 3** Установка и настройка инструментов для анализа защищённости.	2	0	0	0	0	2	0	
1.4	**Самостоятельная работа № 1** Установка систем OWASP 10	2	0	0	0	0	0	2	
1.5	**Самостоятельная работа № 2** Установка систем OSIM	2	0	0	0	0	0	2	
1.6	**Самостоятельная работа № 3** Установка систем мониторинга Zabbix	2	0	0	0	0	0	2	
2	**Модуль 2 Инструменты анализа уязвимостей**	**10**	**0**	**0**	**6**	**0**	**2**	**2**	Практические работы №№3-6 Самостоятельная работа №4
2.1	**Практическая работа № 3** Работа с сетевым трафиком при помощи инструментов типа «снифер».	2	0	0	2	0	0	0	

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
2.2	**Практическая работа №4** Работа с программами анализа защищённости сетевых устройств	2	0	0	2	0	0	0	
2.3	**Практическая работа №5** Работа с сетевым трафиком по модели OWASP 10.	2	0	0	2	0	0	0	
2.4	**Практическая работа № 6** Работа с автоматизированными средствами эксплуатации уязвимостей.	2	0	0	0	0	2	0	
2.5	**Самостоятельная работа № 4** Работа по анализу эксплуатации уязвимостей на основе mutillidae	2	0	0	0	0	0	2	
3	**Модуль 3 Механизмы защиты**	**8**	**0**	**0**	**6**	**0**	**0**	**2**	Практические работы №№7-9 Самостоятельная работа №5
3.1	**Практическая работа № 7** Настройка персональных межсетевых экранов.	2	0	0	2	0	0	0	
3.2	**Практическая работа № 8** Настройка служб на безопасный доступ к системам	2	0	0	2	0	0	0	
3.3	**Практическая работа № 9** Реализация системы мониторинга и оповещения	2	0	0	2	0	0	0	
3.4	**Самостоятельная работа № 5** Настройка встроенных механизмов защиты операционных систем	0	0	0	0	0	0	2	
3.5	Итоговая аттестация	0	0	0	0	0	0	0	**Дифференцированный зачет**
	Итого:	**30**	**0**	**0**	**16**	**0**	**4**	**10**	

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

3.1 Для реализации программы повышения квалификации должны быть предусмотрены следующие специальные помещения:

Мастерская по компетенции Кибер-безопасность, оснащенная оборудованием и техническими и программными средствами обучения:

доска классная – 1 шт., стол компьютерный– 13 шт., стул – 13 шт., компьютерные кресла – 13 шт., системный блок (CPU AMD Ryzen 7 3700x (8 Cores/32MB/8T/3.6GHz); 16 Гбайт (16 Гбайт) памяти DDR4, 2 666 МГц, без ECC; твердотельный накопитель M.2 PCIe NVMe, 512 Гбайт, класс 35) – 13 шт., монитор (Asus 23”8) – 13 шт., клавиатура (Oklick 530S) – 14 шт., мышь для компьютера (Defender OPTICAL MB-160) – 14 шт., источник бесперебойного питания – 13 шт., проектор – 1 шт., активная колонка 1шт., VMware Workstation 15 Professional – 10 шт., офисный пакет Microsoft Office Professional 2016- 13 шт, виртуальный межсетевой экран следующего поколения Cisco Firepower в составе с FMC- 10 шт., ОС Microsoft Windows Server - 1 шт., ОС Microsoft Windows 10 - 13 шт., противошумовые наушники - 10 шт., сервер SuperMicro CSE-113AC2-R706WB2 2x750W black Intel Xeon Silver 4216 256 ГБ ОЗУ, 960 GB SSD 1шт., монитор 23,6 – 1 шт., источник бесперебойного питания для сервера - 1 шт., стойка двухрамная (стк-24.2-9005 цмо) – 1 шт., телевизор на стоике (huawei 55”) – 1 шт., экран для проектора (SAKURA CINEMA WALLSCREEN) – 1 шт., МФУ (Xerox B205) – 1 шт.

3.2 Информационное обеспечение реализации программы

3.2.1. Печатные или электронные издания

1. Баринов, В.В. Компьютерные сети (2-е изд., стер.) : учебник / В.В. Баринов. - Москва: Академия, 2019.
2. Бубнов, А.А. Основы информационной безопасности (3-е изд.) : учебник / А.А. Бубнов. - Москва: Академия, 2020.
3. Бубнов, А.А. Техническая защита информации в объектах информационной инфраструктуры (1-е изд.) : учебник / Бубнов, А.А. - Москва: Академия, 2019.
4. Ворона, В. А. Технические системы охранной и пожарной сигнализации. (Серия «Обеспечение безопасности объектов», выпуск 5) / В. А. Ворона, В. А. Тихонов. - Москва: Горячая Линия - Телеком, 2018.
5. Девицына, С.Н. Монтаж и эксплуатация направляющих систем (1-е изд.): учебник / С.Н. Девицына. - Москва: Академия, 2019.
6. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в ip-сетях в 2 ч. Часть 2 : учебник и практикум для СПО / М. В. Дибров. - Москва: Юрайт, 2020.

7. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в ip-сетях в 2 ч. Часть 1 : учебник и практикум для СПО / М. В. Дибров. - Москва: Юрайт, 2020.

8. Журавлева, Л.В. Электрорадиоизмерения (1-е изд.) : учебник / Л. В. Журавлева. - Москва: Академия,

9. Зверева, В.П. Сопровождение и обслуживание программного обеспечения компьютерных систем (2-е изд., испр.) : учебник / В. П. Зверева - Москва: Академия, 2020.

10. Ильин, М.Е. Криптографическая защита информации в объектах информационной инфраструктуры (1-е изд.) : учебник. / М.Е. Ильин. - Москва: Академия, 2020.

11. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для СПО / О. В. Казарин, А. С. Забабурин. - Москва: Юрайт, 2020.

12. Костров, Б.В. Сети и системы передачи информации (2-е изд., перераб. и доп.) : учебник / Б.В. Костров. - Москва: Академия, 2019.

13. Маркин, А. В. Программирование на SQL : учебное пособие для СПО / А. В. Маркин. - Москва: Юрайт, 2020.

4 ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Форма дифференцированного зачета: дифференцированный зачет проводится по результатам текущего контроля и включает выполненные и оцененные практические работы по программе повышения квалификации «Анализ защищенности информационных систем».

Условия выполнения задания:

Место выполнения задания: учебная аудитория, на последнем учебном занятии по программе повышения квалификации «Анализ защищенности информационных систем».

Критерии оценивания дифференцированного зачета

«Отлично» - практические работы выполнены в полном объёме на «отлично» и «хорошо» с преобладанием отметок «отлично».

«Хорошо» - практические работы выполнены в полном объёме с преобладанием отметок «хорошо».

«Удовлетворительно» - практические работы выполнены с преобладанием отметок «удовлетворительно».

«Неудовлетворительно» - практические работы выполнены не в полном объёме или с преобладанием отметок «неудовлетворительно».