Аннотация

программы дополнительного профессионального образования профессорско-преподавательского состава в области информационной безопасности в рамках реализации федерального проекта «Информационная безопасность»

Наименование: «Защищенные информационные системы»

1.	Наименование образовательной организации	Федеральное государственное бюджетное образовательное учреждение высшего образования Поволжский государственный университет телекоммуникаций и информатики
2.	Наименование программы ДПО (в т.ч. повышение квалификации/профессиональная переподготовка)	Защищенные информационные системы (повышение квалификации)
3.	Объем часов	72,0
4.	Специальность/направление (ФГОС 3++), по которым реализуется программа	10.04.01 Информационная безопасность
5.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	Защищенные информационные системы (обязательная по ФГОС)
6.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	Профстандарт 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях». ОТФ F, F/01.7, ОТФ F F/02.7
7.	Ключевые результаты обучения: (знать, уметь)	
	Знать: уязвимости информационных систем, современные информационные технологии (операционные системы, базы данных, вычислительные сети), методы защиты информации от несанкционированного доступа и специальных программных воздействий на нее; Знать: состояние и перспективы развития систем защиты сетей электросвязи от НСД; основы моделирования ЗТКС и угрозы их информационной безопасности. Уметь: проводить анализ угроз безопасности информации на объекте информатизации; разрабатывать аналитическое обоснование необходимости создания системы защиты информации (модель угроз безопасности информации); разрабатывать эскизный и технический проекты системы защиты информации. Уметь: формировать исходные данные и ограничения при проектировании сети электросвязи, проводить анализ угроз НСД к сети электросвязи.	
8.	Дидактика программы (наименования модулей (дисциплин), разделов (тем).	
	1. Начальные сведения о задачах защищённых информационных систем (ЗИС). Постановка и классификация задач. 2. Безопасность сетей и телекоммуникационных устройств. Безопасность ПО. 3. Безопасность хранения и передачи информации. 4. Методы проектирования и анализа информационных систем. 5. Определение степени защищенности информационной системы. 6. Реализация программ информационной защиты.	
9.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, метод. рекомендации по лаб.работам, фонд оценочных средств.	1. Курс лекций программы ДПО. 2. Методические указания «Методы и средства проектирования информационных систем и технологий. Ч. 1 : Изучение возможностей UML». 3. Оценочные средства ДПО в виде тестирующего комплекса.
10.	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные представители организаций.	Директор специализированного научно-технического центра «Преграда». Эксперт мониторинга киберугроз ПАО «МегаФон».

11.	Используемые отечественные ПО и средства защиты информации (при наличии)	-

Аннотация

программы дополнительного профессионального образования профессорско-преподавательского состава в области информационной безопасности в рамках реализации федерального проекта «Информационная безопасность»

Наименование: «Система управления информационной безопасностью организации в соответствии с требованиями международных и национальных стандартов»

12.	Наименование образовательной организации	Федеральное государственное бюджетное образовательное учреждение высшего образования Поволжский государственный университет телекоммуникаций и информатики
13.	Наименование программы ДПО (в т.ч. повышение квалификации/профессиональная переподготовка)	Система управления информационной безопасностью организации в соответствии с требованиями международных и национальных стандартов (повышение квалификации)
14.	Объем часов	72,0
15.	Специальность/направление (ФГОС 3++), по которым реализуется программа	10.04.01 Информационная безопасность
16.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	Управление информационной безопасностью (обязательная по ФГОС)
17.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	Профстандарт 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», ОТФ D, D/01.7. ОТФ F, F/01.7
18.	Ключевые результаты обучения: (знать, уметь)	
	Знать: модели угроз НСД к сетям электросвязи; методики оценки уязвимостей сетей электросвязи с точки зрения возможности НСД к ним; национальные, межгосударственные и международные стандарты в области защиты информации; Знать: состояние и перспективы развития систем защиты сетей электросвязи от НСД; основы моделирования ЗТКС и угрозы их информационной безопасности; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. Уметь: выявлять и оценивать угрозы НСД к сетям электросвязи; проводить проверку работоспособности и эффективности применяемых программно-аппаратных (в том числе криптографических) и технических средств защиты сетей электросвязи от НСД. Уметь: формировать исходные данные и ограничения при проектировании сети электросвязи, проводить анализ угроз НСД к сети электросвязи; применять методологию менеджмента рисков информационной безопасности в телекоммуникационных системах и сетях электросвязи.	
19.	Дидактика программы (наименования модулей (дисциплин), разделов (тем).	
	7. Классификация и примеры угроз ИБ. 8. Система менеджмента информационной безопасности. Этапы организации системы менеджмента информационной безопасности. 9. Порядок использования политик, руководств, стандартов. 10. Управление ИБ на основе серии стандартов ISO/IEC 27000 (ГОСТ ИСО МЭК 27000): 27001, 27002, 27005. 11. Управление ИБ на основе серии NIST SP 800 series. 12. Мировые практики управления безопасностью.	
20.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, метод. рекомендации по лаб.работам, фонд оценочных средств.	1. Курс лекций программы ДПО. 2. Учебное пособие «Планирование и управление информационной безопасностью». 3. Оценочные средства ДПО в виде тестирующего комплекса.

21.	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные представители организаций.	Директор специализированного научно-технического центра «Преграда» Главный консультант управления информационной безопасности Департамента информационных технологий и связи Самарской области
22.	Используемые отечественные ПО и средства защиты информации (при наличии)	Система автоматизации управления рисками РискМенеджер.

Аннотация

программы дополнительного профессионального образования профессорско-преподавательского состава в области информационной безопасности в рамках реализации федерального проекта «Информационная безопасность»

Наименование: «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»

23.	Наименование образовательной организации	Федеральное государственное бюджетное образовательное учреждение высшего образования Поволжский государственный университет телекоммуникаций и информатики
24.	Наименование программы ДПО (в т. ч. повышение квалификации / профессиональная переподготовка)	Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (профессиональная переподготовка)
25.	Объем часов	606,0
26.	Специальность/направление (ФГОС 3++), по которым реализуется программа	10.03.01 Информационная безопасность
27.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	Техническая защита информации (СибГУТИ, https://sibsutis.ru/sveden/education/3295766/)
28.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	Профстандарт 06.034 «Специалист по технической защите информации»
29.	Ключевые результаты обучения: (знать, уметь)	
	Знать: организацию и планирование работ по ТЗКИ; определение угроз безопасности информации ограниченного доступа; правовые аспекты ТЗКИ; меры и средства ТЗКИ; требования по защите информации и созданию системы ТЗКИ. Уметь: выполнять комплекс работ по созданию системы защиты информации; внедрять меры и средства ТЗКИ.	
30.	Дидактика программы (наименования модулей (дисциплин), разделов (тем).	
	13. Организационно правовые основы ТЗКИ. 14. Аппаратные средства вычислительной техники. 15. Системы и сети передачи информации. 16. Способы и средства ТЗКИ от утечки по техническим каналам. 17. Меры и средства ТЗКИ от несанкционированного доступа. 18. Техническая защита конфиденциальной информации от специальных воздействий. 19. Организация защиты конфиденциальной информации на объектах информатизации. 20. Аттестация объектов информатизации по требованиям безопасности информации. 21. Контроль состояния ТЗКИ.	
31.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, метод. рекомендации по лаб. работам, фонд оценочных средств.	1. Курс лекций программы ДПО «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну». 2. Методические рекомендации к лабораторным работам программы ДПО «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну». 3. Оценочные средства ДПО в виде тестирующего комплекса.
32.	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены	Руководитель управления информационной безопасности Департамента информационных технологий и связи Самарской области

	к реализации программы или отдельные представители организаций.	Директор специализированного научно-технического центра «Преграда» Главный консультант управления информационной безопасности Департамента информационных технологий и связи Самарской области УЦ ИнфоТеКС
33.	Используемые отечественные ПО и средства защиты информации (при наличии)	ST-031 «Пиранья», СВАЗ «Соната», ЛГШ-104 «РаМЗес», ROHDE & SHWAZ FS300, Г4-143 «Катран»

Аннотация

программы дополнительного профессионального образования профессорско-преподавательского состава в области информационной безопасности в рамках реализации федерального проекта «Информационная безопасность»

Наименование: «Технологии и средства защиты компьютерных систем»

34.	Наименование образовательной организации	Федеральное государственное бюджетное образовательное учреждение высшего образования Поволжский государственный университет телекоммуникаций и информатики
35.	Наименование программы ДПО (в т. ч. повышение квалификации / профессиональная переподготовка)	Технологии и средства защиты компьютерных систем (профессиональная переподготовка)
36.	Объем часов	360,0
37.	Специальность/направление (ФГОС 3++), по которым реализуется программа	10.05.01 Компьютерная безопасность 10.05.02 Информационная безопасность телекоммуникационных систем
38.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	Модели безопасности компьютерных систем (ВУЗы: ВШЭ, РУТ (МИИТ), МИРЭА) Защита информационных процессов в компьютерных системах (ВУЗы: ЮФУ,) Защита в операционных системах (ВУЗы: РУТ (МИИТ), МИРЭА)
39.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	Профстандарт 06.032 «Специалист по безопасности компьютерных систем и сетей», ОТФ С, С/01.7
40.	Ключевые результаты обучения: (знать, уметь)	
	Знать: нормативные правовые акты, методические документы и национальные стандарты в области обеспечения информационной безопасности; понятия информации, информационной безопасности, принципы построения современных операционных систем и особенности их применения; принципы построения и функционирования систем и сетей передачи информации; Уметь: соблюдать требования антикоррупционного законодательства, воздерживаться от поведения, вызывающего сомнение в объективном и беспристрастном исполнении должностных (служебных) обязанностей; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; применять математические методы при исследовании криптографических алгоритмов;	
41.	Дидактика программы (наименования модулей (дисциплин), разделов (тем).	
	22. Нормативно правовое регулирование в сфере информационной безопасности. 23. Модели безопасности компьютерных систем. Оценка защищенности компьютерных систем. 24. Криптографические и не криптографические методы и средства защиты компьютерных систем. 25. Защищенные операционные системы. Защита информации в ОС. 26. Построение защищенной компьютерной сети. 27. Защита программ и данных. Гарантированное удаление данных.	
42.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, метод. рекомендации по лаб.работам, фонд оценочных средств.	1. Курс лекций программы ДПО «Технологии и средства защиты компьютерных систем». 2. Методические рекомендации к лабораторным работам программы ДПО «Технологии и средства защиты компьютерных систем». 3. Оценочные средства ДПО в виде тестирующего комплекса.
43.	Фирмы-производители средств защиты информации, внешние образовательные	Руководитель управления информационной безопасности Департамента информационных технологий и связи

	организации, которые будут привлечены к реализации программы или отдельные представители организаций.	Самарской области Директор специализированного научно-технического центра «Преграда» Главный консультант управления информационной безопасности Департамента информационных технологий и связи Самарской области УЦ ИнфоТеКС
44.	Используемые отечественные ПО и средства защиты информации (при наличии)	Антивирус Касперского, Wireshark, Open VAS.

Аннотация

программы дополнительного профессионального образования профессорско-преподавательского состава в области информационной безопасности в рамках реализации федерального проекта «Информационная безопасность»

Наименование: «Тестирование на проникновение»

45.	Наименование образовательной организации	Федеральное государственное бюджетное образовательное учреждение высшего образования Поволжский государственный университет телекоммуникаций и информатики
46.	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Программа повышения квалификации «Тестирование на проникновение»
47.	Объем часов	72,0
48.	Специальность/направление (ФГОС 3++), по которым реализуется программа	10.03.01 Информационная безопасность
49.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	Защита программ и данных (Воронежский институт МВД России), Методы и средства расследования компьютерных инцидентов (Казанский национальный исследовательский технический университет им. А.Н.Туполева-КАИ), Проверка информационной защищенности на соответствие (БашГУ), Методы и инструментальные средства проведения расследования компьютерных инцидентов (Самарский университет)
50.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	Профстандарт 06.032 «Специалист по безопасности компьютерных систем и сетей», ОТФ B, B/02.6
51.	Ключевые результаты обучения: (знать, уметь)	
	Знать: порядок реализации методов и средств межсетевого экранирования; виды политик управления доступом и информационными потоками в компьютерных сетях; источники угроз информационной безопасности; нормативные правовые акты в области защиты информации; организационные меры по защите информации. Уметь: оценивать угрозы безопасности информации в компьютерных сетях; обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях; проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях.	
52.	Дидактика программы (наименования модулей (дисциплин), разделов (тем).	
	28. Сбор информации - необходимый набор инструментов и методик получения информации об объекте тестирования, а также методы противодействия такому сбору и превентивные меры по предотвращению такого рода действий. 29. Web технологии - понимание работы web ресурсов, web серверов, протокола HTTP, языков HTML, DHTML, JS, PHP, SQL, Ajax, API, их уязвимостей и наиболее часто встречающиеся угрозы веб-приложениям, инструменты тестирования. 30. Reverse Engineering - разбор и декомпиляция программ, дизассемблирование с целью определения исходного кода и недекларированных возможностей программного обеспечения. 31. Linux - понимание особенностей работы linux-подобных систем. 32. Сетевая безопасность - снифферы, сетевые протоколы, наиболее часто встречающиеся угрозы, атаки и методы противодействия им. 33. Криптография - алгоритмы шифрования, инструменты шифрования и расшифрования, средства криптоанализа. 34. Стеганография и средства сокрытия факта передачи информации и методы обнаружения такой передачи.	
53.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, метод. рекомендации по	1. Курс лекций программы ДПО «Этичный хакинг» 2. Методические рекомендации к лабораторным работам программы ДПО «Этичный хакинг».

	лаб.работам, фонд оценочных средств.	3. Оценочные средства ДПО в виде тестирующего комплекса.
54.	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные представители организаций.	Руководитель управления информационной безопасности Департамента информационных технологий и связи Самарской области Директор специализированного научно-технического центра «Преграда» Главный консультант управления информационной безопасности Департамента информационных технологий и связи Самарской области
55.	Используемые отечественные ПО и средства защиты информации (при наличии)	Linux Kali, VirtualBox, Metasploit Framework, John The Ripper, Wireshark, Aircrack-ng, Nmap, SuperScan, Reaver, Routerpwn, Homedale, Keylogger