Аннотация

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

Наименование: «Безопасность вычислительных сетей»

1.	Наименование образовательной организации-разработчика программы	Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ)
2.	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Программа повышения квалификации «Безопасность вычислительных сетей»
3.	Объем часов	72
4.	Специальность/направление (ФГОС 3++), по которым реализуется программа	10.05.02 Информационная безопасность телекоммуникационных систем
5.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	Безопасность вычислительных сетей
6.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	06.032 Профессиональный стандарт "Специалист по безопасности компьютерных систем и сетей"
7.	Ключевые результаты обучения: (знать, уметь)	
	Знать: - Актуальные угрозы информационной безопасности - Сетевые атаки канального уровня - Принципы работы межсетевых экранов - Методы сканирования и перехвата трафика - Принципы работы систем предотвращения вторжений и аномалий - Принципы построения виртуальных частных туннелей (VPN) Уметь: - Предотвращать атаки вида отказ в облуживании (DoS) - Настраивать системы предотвращения вторжений и аномалий - Искать и предотвращать киберинциденты в компьютерных сетях Владеть навыками: - Навыками настройки VPN - Навыками настройки межсетевых экранов	
8.	Дидактика программы (наименования модулей (дисциплин), разделов (тем).	
	Модуль «Безопасность вычислительных сетей» - Актуальные угрозы сетевой безопасности - Изучение сетевых компьютерных атак канального уровня - Сетевые компьютерные атаки канального уровня - Защита маршрутизаторов. Безопасность протоколов динамической маршрутизации - Виртуальные частные сети VPN - Межсетевые экраны - Системы предотвращения вторжений и аномалий - Сканирование и перехват трафика - Отказы в обслуживании - Поиск и предотвращение киберинцидентов в компьютерных сетях	
9.	Планируемое обеспечение программы	1. Курс лекций программы ДПО «Безопасность

	(УМК), перечислить: курс лекций, учебное пособие, метод рекомендации по лаб.работам, фонд оценочных средств.	вычислительных сетей». 2. Учебное пособие «Безопасность вычислительных сетей». 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.	Управление ФСТЭК по СЗФО АО «Информационные Технологии и Коммуникационные Системы» («ИнфоТеКС») Национальный киберполигон Лаборатория ППШ
11.	Используемые отечественные ПО и средства защиты информации (при наличии)	АО «Информационные Технологии и Коммуникационные Системы» («ИнфоТеКС», PositiveTechnologies, КодБезопасности, Конфидент

Аннотация

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

Наименование: «Подготовка специалистов для решения задач в области обеспечения безопасности значимых объектов КИИ»

1.	Наименование образовательной организации-разработчика программы	Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ)
2.	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Программа повышения квалификации «Подготовка специалистов для решения задач в области обеспечения безопасности значимых объектов КИИ»
3.	Объем часов	72
4.	Специальность/направление (ФГОС 3++), по которым реализуется программа	10.05.02 Информационная безопасность телекоммуникационных систем
5.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)
6.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	06.032 Профессиональный стандарт "Специалист по безопасности компьютерных систем и сетей"
7.	Ключевые результаты обучения: (знать, уметь)	
	Знать: - нормативные правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ; - основы функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации; - основные понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ; - принципы организации систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования; - процедуру категорирования объектов КИИ, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов КИИ; - основные принципы выявления наличия критических процессов у субъекта КИИ; - основные принципы выявления объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов; - процедуры выявления и анализа угроз безопасности информации, обрабатываемой объектом КИИ; - общие требования по обеспечению безопасности значимых объектов КИИ; - общие требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования; - требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ; - требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ;	

	- цели, задачи, основные принципы организации государственного контроля в области обеспечения безопасности значимых объектов КИИ; - порядок обработки результатов контроля (проверки) состояния безопасности значимых объектов КИИ Уметь: - определять категории значимости объектов КИИ; - формировать сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий; - выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности и последствий от их реализации; - обосновывать организационные и технические меры, подлежащие реализации в рамках системы безопасности значимого объекта КИИ; - определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер в рамках системы безопасности значимого объекта КИИ; - определять структуру системы безопасности значимого объекта КИИ; - осуществлять выбор средств защиты информации с учетом их стоимости, совместимости с применяемыми программными и программно-аппаратными средствами, функций безопасности этих средств и особенностей их реализации, а также категории значимого объекта КИИ; -определять требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации; - определять требования к обеспечению безопасности значимого объекта КИИ Владеть навыками: - работы с нормативными правовыми актами, методическими документами в области обеспечения безопасности значимых объектов КИИ; - работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения значимых объектов КИИ, в том числе зарубежными информационными ресурсами; - разработки организационно-распорядительных документов по безопасности значимых объектов КИИ; - эксплуатации системы безопасности значимого объекта КИИ; - выявления угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ; - участия в разработке организационных и технических мероприятий по защите объектов КИИ; - установки, настройки и применения современных средств защиты информации, обрабатываемой объектами КИИ; - проведения работ по контролю состояния безопасности объектов КИИ.
8.	Дидактика программы (наименования модулей (дисциплин), разделов (тем).
	Учебный модуль №1. Основы обеспечения безопасности значимых объектов КИИ Тема №1. Правовые основы обеспечения безопасности КИИ Российской Федерации Тема №2. Угрозы безопасности информации, обрабатываемой на объектах КИИ Учебный модуль №2. Организация работ по обеспечению безопасности значимого объекта КИИ Тема №1. Категорирование объектов КИИ Тема №2. Требования по обеспечению безопасности значимых объектов КИИ Тема №3. Система безопасности значимого объекта КИИ Тема №4. Стадии (этапы) работ по созданию систем безопасности Учебный модуль №3. Контроль за обеспечением безопасности значимого объекта КИИ Тема №1. Контроль за обеспечением безопасности значимого объекта КИИ Тема №2. Правовая основа создания и функционирования ГосСОПКА, структура, субъекты

	взаимоотношений	
9.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, метод рекомендации по лаб.работам, фонд оценочных средств.	1. Курс лекций программы ДПО «Подготовка специалистов для решения задач в области обеспечения безопасности значимых объектов КИИ». 2. Учебное пособие «Подготовка специалистов для решения задач в области обеспечения безопасности значимых объектов КИИ». 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.	Управление ФСТЭК по СЗФО АО «Информационные Технологии и Коммуникационные Системы» («ИнфоТеКС») Национальный киберполигон Лаборатория ППШ КодБезопасности Конфидент PositiveTechnologies
11.	Используемые отечественные ПО и средства защиты информации (при наличии)	программа ScanOVAL; дистрибутив Kali Linux; система обнаружения вторжений DallasLock; - межсетевой экран DallasLock; - антивирусная программа Dr.Web; - программный комплекс защиты информации DallasLock К

Аннотация

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

Наименование: «Комплексная защита объектов информатизации»

1.	Наименование образовательной организации-разработчика программы	Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ)
2.	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Профессиональная переподготовка «Комплексная защита объектов информатизации»
3.	Объем часов	360
4.	Специальность/направление (ФГОС 3++), по которым реализуется программа	10.05.02 Информационная безопасность телекоммуникационных систем
5.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	Комплексная защита объектов информатизации
6.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	06.032 Профессиональный стандарт "Специалист по безопасности компьютерных систем и сетей"
7.	Ключевые результаты обучения: (знать, уметь)	
	Знать: - нормативные правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ; - основы функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации; - основные понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ; - принципы организации систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования; - процедуру категорирования объектов КИИ, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов КИИ; - основные принципы выявления наличия критических процессов у субъекта КИИ; - основные принципы выявления объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов; - процедуры выявления и анализа угроз безопасности информации, обрабатываемой объектом КИИ; - общие требования по обеспечению безопасности значимых объектов КИИ; - общие требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования; - требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ; - требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ; - цели, задачи, основные принципы организации государственного контроля в области обеспечения безопасности значимых объектов КИИ; - порядок обработки результатов контроля (проверки) состояния безопасности значимых объектов КИИ.	

- основные методы проведения инструментального мониторинга качества обслуживания в телекоммуникационных системах и сетях в целях управления их функционированием
- основные угрозы элементов информационно-телекоммуникационной инфраструктуры
- этапы жизненного цикла проекта;
- этапы разработки и реализации проекта;
- методы разработки и управления проектами
- модели OSI и TCP/IP
- принципы работы протоколов Ethernet, IPv4, IPv6, TCP, UDP, ICMP
- принципы работы протокола связующего дерева Spanning Tree (RSTP, MST).\
- устройство протоколов VRRP, GLBP
- принципы работы протоколов динамической маршрутизации OSPF, BGP
- принципы построения агрегированных каналов EtherChannel
- основы виртуализации в компьютерных сетях
- принципы построения VLAN, магистральных интерфейсов и основы маршрутизации между VLAN
- способы обеспечения безопасности коммутатора

Уметь:
- определять категории значимости объектов КИИ;
- формировать сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий;
- выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности и последствий от их реализации;
- обосновывать организационные и технические меры, подлежащие реализации в рамках системы безопасности значимого объекта КИИ;
- определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер в рамках системы безопасности значимого объекта КИИ;
- определять структуру системы безопасности значимого объекта КИИ;
- осуществлять выбор средств защиты информации с учетом их стоимости, совместимости с применяемыми программными и программно-аппаратными средствами, функций безопасности этих средств и особенностей их реализации, а также категории значимого объекта КИИ;
-определять требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации;
- определять требования к обеспечению безопасности значимого объекта КИИ
- проводить инструментальный мониторинг качества обслуживания в телекоммуникационных системах и сетях в целях управления их функционированием
- анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности.
- разрабатывать проект с учетом анализа альтернативных вариантов его реализации, определять целевые этапы, основные направления работ;
- объяснить цели и сформулировать задачи, связанные с подготовкой и реализацией проекта-управлять проектом на всех этапах его жизненного цикла.
- настраивать протоколы динамической маршрутизации: OSPF, BGP, IS-IS
- настраивать протоколы RSTP, MST
- настраивать протокол EtherChannel

Владеть:
- навыками работы с нормативными правовыми актами, методическими документами в области обеспечения безопасности значимых объектов КИИ;
- навыками работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения значимых объектов КИИ, в том

	числе зарубежными информационными ресурсами; - навыками разработки организационно-распорядительных документов по безопасности значимых объектов КИИ; - навыками эксплуатации системы безопасности значимого объекта КИИ; - навыками выявления угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ; - навыками участия в разработке организационных и технических мероприятий по защите объектов КИИ; - навыками установки, настройки и применения современных средств защиты информации, обрабатываемой объектами КИИ; - навыками проведения работ по контролю состояния безопасности объектов КИИ - навыками проведения анализа защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием - навыками оценки технических возможностей рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности - методиками разработки и управления проектом; - методами оценки потребности в ресурсах и эффективности проекта навыками настройки VLAN, магистральных интерфейсов и маршрутизации между VLAN - навыками настройки функций обеспечения безопасности коммутатора
8.	Дидактика программы (наименования модулей (дисциплин), разделов (тем).
	Учебный модуль №1. Основы обеспечения безопасности значимых объектов КИИ Правовые основы обеспечения безопасности КИИ Российской Федерации Угрозы безопасности информации, обрабатываемой на объектах КИИ **Учебный модуль №2. Организация работ по обеспечению безопасности значимого объекта КИИ** Категорирование объектов КИИ Требования по обеспечению безопасности значимых объектов КИИ Система безопасности значимого объекта КИИ Стадии (этапы) работ по созданию систем безопасности **Учебный модуль №3. Контроль за обеспечением безопасности значимого объекта КИИ** Контроль за обеспечением безопасности значимого объекта КИИ Правовая основа создания и функционирования ГосСОПКА, структура, субъекты взаимоотношений **Учебный модуль №4. Сети и системы передачи информации** Введение в коммутируемые и маршрутизируемые сети Принципы коммутации в компьютерных сетях Сети VLAN Маршрутизация между виртуальными локальными сетями Статическая маршрутизация Динамическая маршрутизация Протокол динамической маршрутизации OSPF Протоколы динамической маршрутизации IBGP, EBGP Протокол динамической маршрутизации IS-IS Основные принципы обеспечения безопасности компьютерных сетей **Учебный модуль №5. Тестирование на проникновение и этичный хакинг** Сканирование и рекогносцировка в сетевой IP-инфраструктуре Основные методы поиска уязвимостей операционных систем (Windows, Linux, MacOS) Основные методы перехвата трафика на канальном и сетевом уровне, в соответствии со стеком протоколов TCP/IP. Проведение атак типа «Отказ в обслуживании» и «Распределенный отказ в обслуживании». Основные методы поиска уязвимостей в реализации протоколов сетевого и транспортного уровней, в соответствии со стеком протоколов TCP/IP. Эксплуатация уязвимостей WEB-сервисов и приложений Поиск и эксплуатация уязвимостей беспроводных сетей, работающих по стандарту 802.11

	Поиск уязвимостей в мобильных устройствах Методы обхода систем предотвращения вторжений и межсетевых экранов Использование вирусов, закладок в коде. Переполнение буфера Поиск уязвимостей в реализациях криптографических алгоритмов Методы сокрытия деятельности в сети **Учебный модуль №6. Сертификация средств защиты информации** Законодательные, нормативные правовые акты, стандарты и методические документы, регламентирующие проведение работ по оценке соответствия требованиям по безопасности информации продукции. Организационная структура Системы сертификации ФСТЭК России. Программа и методика испытаний. Подготовка к проведению сертификационных испытаний Требования к разработке профилей защиты и заданий по безопасности Порядок проведения испытаний на соответствие техническим условиям Экспертный, статический, динамический, комбинированный и ручной анализы. Требования по разработке отчетных материалов по результатам сертификационных испытаний. Содержание протоколов, заключений. Экспертиза материалов сертификационных испытаний. Аттестация объектов информатизации. Порядок проведения аттестационных испытаний **Учебный модуль №7. Цифровая криминалистика** Введение в цифровые доказательства Работа с данными. Создание образа для цифровой форензики. Работа с жесткими дисками. Файловые системы Анализ работы операционных систем на примере семейства ОС Windows Анализ интернет приложений ОС Windows Анализ уязвимостей ОС Linux, MacOS Анализ уязвимостей MacOS Сетевая форензика Форензика в реальном времени Форензика SSD Форензика памяти	
9.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, метод рекомендации по лаб.работам, фонд оценочных средств.	1. Курс лекций программы ДПО «Комплексная защита объектов информатизации». 2. Учебное пособие «Комплексная защита объектов информатизации». 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.	Управление ФСТЭК по СЗФО АО «Информационные Технологии и Коммуникационные Системы» («ИнфоТеКС») Национальный киберполигон Лаборатория ППШ КодБезопасности Конфидент PositiveTechnologies
11.	Используемые отечественные ПО и средства защиты информации (при наличии)	программа ScanOVAL; дистрибутив Kali Linux; система обнаружения вторжений DallasLock; - межсетевой экран DallasLock; - антивирусная программа Dr.Web; - программный комплекс защиты информации DallasLock K

Аннотация

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

Наименование: «Преподаватель высшей школы в области информационной безопасности»

1.	Наименование образовательной организации-разработчика программы	Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ)
2.	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Профессиональная переподготовка «Преподаватель высшей школы в области информационной безопасности»
3.	Объем часов	360
4.	Специальность/направление (ФГОС 3++), по которым реализуется программа	10.04.01 Информационная безопасность
5.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	Педагогическая практика
6.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	01.010. Профессиональный стандарт «Руководитель образовательной организации высшего образования», ТФ Б. Координация деятельности по формированию и реализации стратегии развития образовательной организации высшего образования
7.	Ключевые результаты обучения: (знать, уметь)	
	Знать: - нормативные правовые акты в области ИБ - особенности реализации учебного процесса с использованием методических материалов основных регуляторов в области ИБ - особенности проведения экспертизы материалов в целях открытого опубликования - законы в сфере образования - особенности нормативно-правового обеспечения учебного процесса - ФГОС по направлениям подготовки 10.00.00 Информационная безопасность - профессиональные стандарты в области ИБ - процедуру лицензирования, аккредитации, проведения конкурса КЦП - системы организации онлайн тестирования - программно-аппаратные средства защиты информации - программные среды для эмуляции оборудования - программные продукты для проведения занятий в режиме ДОТ - устройство Национального киберполигона - особенности организации учебного процесса по сетевым дисциплинам - особенности организации учебного процесса по технической защите информации - особенности организации учебного процесса по организационно-правовым аспектам ИБ - особенности организации учебного процесса по компьютерным дисциплинам - Категориальный аппарат педагогики Уметь: - проектировать ООП - работать в программных средах эмуляции оборудования	

	- проводить типовые сценарии атак на базе Национального киберполигона - использовать программные продукты для проведения занятий в режиме ДОТ - проводить оценку воспитательной работы преподавателя Владеть навыками: - навыками внедрения отечественного оборудования в учебный процесс; - навыками организации удаленного доступа к оборудованию для проведения лабораторных работ - навыками противодействия киберугрозам
8.	Дидактика программы (наименования модулей (дисциплин), разделов (тем). **Учебный модуль № 1. Государственная система защиты информации, роль образовательных организаций в ней** Государственная система защита информации. Оформление документов в рамках совершенствования системы ГСЗИ от организаций, осуществляющих образовательную деятельность **Учебный модуль № 2. Система нормативных правовых актов РФ в области ИБ, документы, возможные к использованию в преподавательской деятельности** Нормативные правовые акты в области ИБ. Реализация учебного процесса с использованием методических материалов основных регуляторов в области ИБ **Учебный модуль № 3. Организация и контроль состояния системы защиты информации в образовательных организациях** Организация системы защиты информации в образовательных организациях. Вопросы организации внутреннего контроля **Учебный модуль № 4. Экспортный контроль** Экспертиза материалов в целях открытого опубликования **Учебный модуль № 5. Нормативно-правовое обеспечение образования** Законы в сфере образования, нормативно-правовое обеспечение учебного процесса **Учебный модуль № 6. Проектирование ООП** ФГОС по направлениям подготовки 10.00.00 Информационная безопасность, профессиональные стандарты в области ИБ, методология проектирования ООП **Учебный модуль № 7. Контрольно-надзорные мероприятия в сфере образования** Лицензирование, аккредитация, конкурс КЦП **Учебный модуль № 8. Организация тестирования остаточных знаний.** Системы онлайн тестирования. Moodle. **Учебный модуль № 9. Вопросы импортозамещения в учебном процессе.** Использование отечественных вендоров для организации обучения. **Учебный модуль № 10. Цифровые двойники в учебном процессе** Программные среды для эмуляции оборудования. EVE-NG, GNS-3. **Учебный модуль № 11. Дистанционные образовательные технологии** Использование программных продуктов для проведения занятий в режиме ДОТ. Использование виртуальных образов оборудования для проведения лабораторных работ. Организация удаленного доступа к оборудованию для проведения лабораторных работ **Учебный модуль № 12. Национальный киберполигон в учебном процессе.** Использование национального киберполигона для проведения лабораторных занятий. Подключение к национальному киберполигону. Состав национального киберполигона **Учебный модуль № 13. Практика преподавания дисциплин. Сетевые технологии** Организация учебного процесса. Проведение занятий по сетевым технологиям с использованием отечественного ПО **Учебный модуль № 14. Практика преподавания дисциплин. Техническая защита информации** Организация учебного процесса. Требования по обеспечению закрытых дисциплин Оценка рисков информационной безопасности. Управление рисками ИБ **Учебный модуль № 15. Практика преподавания дисциплин. Организационно-правовые аспекты ИБ** Организация учебного процесса Введение. Персональные данные на предприятии

	Основные понятия законодательства в сфере персональных данных Работа с персональными данными на предприятии Техническая защита персональных данных в информационных системах Лицензирование деятельности по технической защите конфиденциальной информации Аутсорсинг обработки персональных данных и их технической защиты Контроль и надзор за соблюдением законодательства о персональных данных **Учебный модуль № 16. Практика преподавания компьютерных дисциплин. Безопасность Astra Linux** Организация учебного процесса, установка образов виртуальных машин. Средства организации ЕПП Защищенная графическая подсистема Защищенная система СУБД Средства контроля целостности пакетов Резервное копирование и восстановление данных Модели разграничения доступ Защита от отчуждаемого физического носителя **Учебный модуль № 17. Педагогика высшей школы** Педагогика как наука Категориальный аппарат педагогики Методология педагогической науки Целостность педагогического процесса, его закономерности и этапы Педагогическое мастерство преподавателя в вузе как наставника и воспитателя студентов. Формы и методы воспитательной работы со студентами. Оценка воспитательной работы преподавателя	
9.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, метод рекомендации по лаб.работам, фонд оценочных средств.	1. Курс лекций программы ДПО «Преподаватель высшей школы в области информационной безопасности». 2. Учебное пособие «Преподаватель высшей школы в области информационной безопасности». 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.	Управление ФСТЭК по СЗФО АО «Информационные Технологии и Коммуникационные Системы» («ИнфоТеКС») Национальный киберполигон Лаборатория ППШ КодБезопасности Конфидент PositiveTechnologies
11.	Используемые отечественные ПО и средства защиты информации (при наличии)	программа ScanOVAL; дистрибутив Kali Linux; система обнаружения вторжений DallasLock; - межсетевой экран DallasLock; - антивирусная программа Dr.Web; - программный комплекс защиты информации DallasLock К