ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Уральский государственный университет путей сообщения»
(ФГБОУ ВПО УрГУПС)
Академия корпоративного образования (АКО)
Институт дополнительного профессионального образования (ИДПО)

УТВЕРЖДАЮ:
Директор АКО УрГУПС

_____ И.Л.Васильев
«___» _____ 2013 г.

МОДУЛЬНАЯ ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

(программа повышения квалификации)

«Информационная безопасность»

(название программы)

(по профилю основной профессиональной образовательной программы вуза
090103)
(код программы)

Екатеринбург, 2013

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Уральский государственный университет путей сообщения»
(ФГБОУ ВПО УрГУПС)
Академия корпоративного образования (АКО)
Институт дополнительного профессионального образования (ИДПО)

УТВЕРЖДАЮ:
Директор АКО

_____ И.Л.Васильев
«_____» _____ 2013 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА (МОДУЛЬНАЯ)

(программа повышения квалификации)

«Информационная безопасность»

(название программы)

(по профилю основной профессиональной образовательной программы вуза
***090103*)**
(код программы)

Екатеринбург, 2013

Содержание

Введение

Настоящая дополнительная профессиональная программа (ДПП) предназначена для дополнительного профессионального образования путем освоения программы повышения квалификации (ПК), профессиональной переподготовки (ПП) различных категорий руководителей и специалистов органов государственной власти, предприятий, организаций, учреждений.

ДПП разрабатывается в ИДПО АКО УрГУПС и утверждается только директором АКО, если иное не установлено законом от 29.12.12 № 273-ФЗ.

Данная ДПП является модульной, то есть состоящей из нескольких модулей.

Модуль ДПП — это относительно самостоятельная часть программы, в которой представлена значительная по объему теоретическая и практическая информация по одному из разделов ДПП. Модуль имеет нумерацию, состоящую из одного числа. (Например, *1. Теория информационной безопасности и методология защиты информации*).

Каждый модуль разбит на темы.

Тема модуля ДПП — это минимальный элемент модуля, в котором представлена теоретическая и практическая информация по какой-то его части. Тема имеет нумерацию, состоящую из двух чисел: первое — номер модуля, второе — номер темы в модуле. (Например, *1.3. Государственное регулирование в информационной сфере*).

Каждая тема имеет **содержание**, в котором отражается узкопрофессиональная информация, конкретное умение или навык, тот или иной теоретический вопрос. (Например, *Основные принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации. Информация как объект правовых отношений. Обладатель информации. Право на доступ к информации. Ограничение доступа к информации. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации*).

Минимальный срок освоения темы — 2 часа. Максимальный срок — определяется заказчиком.

Варьируя различными комбинациями тем, на основе модульной ДПП могут быть созданы различные рабочие программы ПК (Приложение А).

Рабочая программа ПК минимально должна состоять из учебно-тематического плана и календарного учебного графика.

Учебно-тематический план рабочей программы ПК разрабатывается на основании тем модулей ДПП заказчиком и исполнителем совместно в соответствии с законами РФ и требованиями заказчика (Приложение Б). План должен содержать:

1) категорию слушателей;
2) форму обучения;
3) трудоемкость;
4) срок освоения;

5) режим занятий;
6) перечень тем модулей ДПП с указанием числа часов и видов занятий;
7) форму аттестации

Календарный учебный график составляется в соответствии с формой обучения, трудоемкостью и сроками освоения на каждый рабочий день (РД) занятий (Приложение В).

1 Общие положения

1.1 Категории слушателей

- Руководители, главные специалисты, начальники подразделений защиты информации аппаратов органов государственной власти.
- Специалисты органов государственной власти по защите информации, осуществляющие разработку и эксплуатацию автоматизированных информационных систем, обеспечивающих обработку, хранение и передачу персональных данных.
- Руководители, главные специалисты, начальники подразделений защиты информации предприятий (организаций, учреждений).
- Специалисты по защите информации (по технической защите информации).
- Специалисты по защите информации (по оценке и аудиту).
- Специалисты по защите информации (по лицензированию и сертификации).
- Руководители, инженерно-технические работники, научные работники научно-исследовательских институтов, конструкторских, изыскательских, проектных организаций.

1.2 Формы обучения

- очная;
- очно-заочная (с применением дистанционных образовательных технологий);
- заочная (с применением дистанционных образовательных технологий).

1.3 Трудоемкость

Для программ повышения квалификации – не менее 40 часов.
Для программ профессиональной переподготовки – не менее 360 часов.

1.4 Сроки освоения

- Для программ повышения квалификации – не менее 2 дней.

- Для программ повышения квалификации с применением дистанционных обучающих технологий – не менее 12 дней (10 дней заочного обучения и 2 дня очного обучения).

- Для программ профессиональной переподготовки – не менее 30 дней.

- Для программ профессиональной переподготовки с применением дистанционных обучающих технологий – не менее 120 дней (90 дней заочного обучения и 30 дней очного обучения).

1.5 Режим занятий

6-8(10) академических (45 мин.) часов в день.

2 Цель

Освоение специалистами актуальных изменений в области информационной безопасности, обновление их теоретических знаний и умений, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению информационной безопасности.

3 Планируемый результат обучения

В результате освоения программы ПК слушателей должны:

ЗНАТЬ:

- содержание основных нормативных правовых актов, регламентирующих вопросы обеспечения информационной безопасности;
- основные виды угроз информационной безопасности;
- содержание и порядок организации работ по обеспечению информационной безопасности;
- процедуры задания и реализации требований по защите информации;
- меры обеспечения информационной безопасности.

УМЕТЬ:

- планировать мероприятия по обеспечению информационной безопасности;
- разрабатывать необходимые документы в интересах организации работ по обеспечению информационной безопасности;
- обосновывать и задавать требования по обеспечению информационной безопасности;
- проводить оценки актуальных угроз информационной безопасности;

- определять состав и содержание мер по обеспечению информационной безопасности, необходимых для блокирования угроз информационной безопасности.

БЫТЬ ОЗНАКОМЛЕНЫ С:

- нормативными правовыми и организационными основами защиты информации в Российской Федерации;
- порядком организации и проведения лицензирования деятельности в области защиты информации;
- документами национальной системы стандартизации, действующими в области защиты информации.

СОВЕРШЕНСТВОВАТЬ (ПОЛУЧИТЬ НОВЫЕ) КОМПЕТЕНЦИИ:

Общепрофессиональные:

- способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;
- способность понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;
- способность использовать нормативные правовые документы в своей профессиональной деятельности;
- способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;
- способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;
- способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов;
- способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия.

Эксплуатационная деятельность:

- способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;

- способностью администрировать подсистемы информационной безопасности объекта;

- способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации.

Проектно-технологическая деятельность:

- способность участвовать в разработке подсистемы управления информационной безопасностью;

- способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;

- способность оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

- способность применять программные средства системного, прикладного и специального назначения;

- способностью использовать инструментальные средства и системы программирования для решения профессиональных задач;

- способность к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

- способность собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.

Экспериментально-исследовательская деятельность:

- способность составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

- способность применять методы анализа изучаемых явлений, процессов и проектных решений;

- способность проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;

- способность проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

- способность принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;

- способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

Организационно-управленческая деятельность:

- способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью;

- способность формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью;

- способность принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

- способность изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации;

- способность участвовать в работах по реализации политики информационной безопасности;

- способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности;

- способность организовать работу малого коллектива исполнителей с учетом требований защиты информации;

- способность организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации;

- способность организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю
.

4 Рабочие программы модулей, учебных предметов, курсов, дисциплин

4.1 Модули ДПП

Модуль 1
Теория информационной безопасности и методология защиты информации

Код Темы	Наименование темы	Для включения в учебно - тематический план (объем часов)
1.1.	Информационная безопасность Российской Федерации	8
1.2.	Организационная основа системы обеспечения информационной безопасности Российской Федерации	8
1.3.	Государственное регулирование в информационной сфере	8
1.4.	Информация ограниченного доступа	8
1.5.	Организация режима коммерческой тайны на предприятии	8
1.6.	Выявление угроз безопасности информации на объектах информатизации	4
1.7.	Защита информации ограниченного доступа	8

Код Темы	Наименование темы	Для включения в учебно - тематиче-ский план (объем часов)
1.8.	Разработка политики безопасности	12

Модуль 2
Физические основы защиты информации

Код Темы	Наименование темы	Для включения в учебно – тематиче-ский план (объем часов)
2.1.	Информационные характеристики полей и сигналов	4
2.2.	Звуковые волны	4
2.3.	Анализ цепей переменного тока	4
2.4.	Анализ эквивалентных схем каналов утечки информации	4
2.5.	Образование каналов утечки информации по цепям пита-ния и заземления	4
2.6.	Электрические фильтры	4
2.7.	Экранирование электрических и магнитных полей	4
2.8.	Излучение электромагнитных волн	4

Модуль 3
Математические основы защиты информации

Код Темы	Наименование темы	Для включения в учебно – тематиче-ский план (объем часов)
3.1.	История развития математических основ криптографии. Шифры	4
3.2.	Алгоритм шифрования DES (Data Encryption Standard)	4
3.3.	Совершенные шифры	4

Код Темы	Наименование темы	Для включения в учебно – тематический план (объем часов)
3.4.	Современное развитие совершенных шифров	4
3.5.	Элементы алгебры и теории чисел в криптографии	4
3.6.	Схемы разделения секрета	4

Модуль 4
Правовое обеспечение информационной безопасности

Код Темы	Наименование темы	Для включения в учебно – тематический план (объем часов)
4.1.	Методы правового регулирования в области информационной безопасности	8
4.2.	Государственное регулирование в области информационной безопасности	8
4.3.	Правовое обеспечение защиты государственной тайны	8
4.4.	Правовое обеспечение защиты информации конфиденциального характера	12
4.5.	Подтверждение соответствия и сертификация	8
4.6.	Организация и проведение лицензирования деятельности по осуществлению мероприятий по оказанию услуг в области технической защиты информации	12
4.7.	Правовые основы организации технической защиты информации ограниченного доступа	8

Модуль 5
Организационное обеспечение информационной безопасности

Код Темы	Наименование темы	Для включения в учебно – тематический план (объем часов)
5.1.	Организационное обеспечение защиты персональных данных на предприятии	8
5.2.	Формирование пакета основных правил, инструкций, требований по обеспечению безопасности предприятия	8
5.3.	Государственная политика информационной безопасности	8
5.4.	Защита информации на предприятии	12
5.5.	Методические рекомендации по подготовке и составлению Положения о подразделении по защите информации	8
5.6.	Оценка эффективности защиты информации	12
5.7.	Контроль состояния защиты информационных ресурсов субъектов Российской Федерации	8
5.8.	Аттестация объектов информатизации по требованиям безопасности информации	2
5.9.	Организация технической защиты информации ограниченного доступа на предприятии	12

Модуль 6
Документоведение

Код Темы	Наименование темы	Для включения в учебно - тематический план (объем часов)
6.1.	Основные виды документов	8
6.2.	Нормативно-методическая база делопроизводства	8
6.3.	Система организационно-правовой документации	8
6.4.	Основные управленческие документы	12
6.5.	Язык и стиль служебных документов	8
6.6.	Систематизация документов	12
6.7.	Делопроизводство и документооборот	8

Модуль 7
Инженерно-техническая защита информации

Код Темы	Наименование темы	Для включения в учебно - тематический план (объем часов)
7.1.	Информация как предмет защиты	8
7.2.	Демаскирующие признаки объектов защиты	8
7.3.	Задачи инженерно-технической защиты информации	8
7.4.	Принципы инженерно-технической защиты информации	8
7.5.	Способы и средства технической защиты информации	12
7.6.	Системы охранно-тревожной сигнализации	8
7.7.	Системы контроля и разграничения доступа	8
7.8.	Функциональная организация систем контроля и управления доступом	8
7.9.	Правовые и организационные вопросы технической защиты информации ограниченного доступа	8
7.10.	Технические средства защиты информации от несанкционированного доступа	4
7.11.	Методы и средства контроля состояния технической защиты информации на объектах информатизации	12

Модуль 8
Программно-аппаратная защита информации

Код Темы	Наименование темы	Для включения в учебно - тематический план (объем часов)
8.1.	Принципы многоуровневой защиты корпоративной информации	8
8.2.	Основы сетевого и межсетевого взаимодействия	12
8.3.	Политика безопасности	8
8.4.	Управление рисками	8
8.5.	Вредоносные программы	8
8.6.	Технологии защиты от вредоносных программ и спама	8

Код Темы	Наименование темы	Для включения в учебно - тематический план (объем часов)
8.7.	Удаленные сетевые атаки	8
8.8.	Системы обнаружения вторжений	8
8.9.	Программные средства защиты информации от несанкционированного доступа	4

Модуль 9
Проектирование систем защиты информации

Код Темы	Наименование темы	Для включения в учебно - тематический план (объем часов)
9.1.	Жизненный цикл автоматизированных систем	4
9.2.	Классификация автоматизированных систем и требования по защите информации	4
9.3.	Средства вычислительной техники. Показатели защищенности от несанкционированного доступа к информации	4
9.4.	Межсетевые экраны. Показатели защищенности от несанкционированного доступа к информации	4
9.5.	Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей	4
9.6.	Испытания автоматизированных систем	4
9.7.	Техническое задание на систему защиты информации	4
9.8.	Основы проектирования и эксплуатации защищенных объектов информатизации	12

Модуль 10
Безопасность операционных систем

Код Темы	Наименование темы	Для включения в учебно - тематиче-ский план (объем часов)
10.1.	Структура операционных систем	4
10.2.	Управление процессами в операционных системах	4
10.3.	Управление памятью в операционных системах	4
10.4.	Устройства ввода-вывода в операционных системах	4
10.5.	Файловые системы в операционных системах	4
10.6.	Защита памяти в операционных системах	4

Модуль 11
Защита и обработка конфиденциальных документов

Код Темы	Наименование темы	Для включения в учебно - тематиче-ский план (объем часов)
11.1.	Конфиденциальность документов	8
11.2.	Организация конфиденциального делопроизводства	12
11.3.	Структура защищенного документооборота	8
11.4.	Виды учета конфиденциальных документов	8
11.5.	Разрешительная система доступа к конфиденциальным документам	8
11.6.	Обработка изданных конфиденциальных документов, си-стематизация документов	8
11.7.	Проверки наличия конфиденциальных документов, уни-чтожение носителей конфиденциальной информации, режим хранения	8
11.8.	Защита конфиденциальной информации в системе элек-тронного документооборота	8

Модуль 12
Защита интеллектуальной собственности и патентоведение

Код Темы	Наименование темы	Для включения в учебно - тематический план (объем часов)
12.1.	Основные понятия интеллектуальной деятельности	8
12.2.	Сущность и содержание понятия объекта интеллектуальной собственности	8
12.3.	Объекты интеллектуальной собственности, охраняемые авторским правом	12
12.4.	Особенности некоторых произведений как объектов авторского права	8
12.5.	Объекты интеллектуальной собственности, охраняемые смежным правом	12
12.6.	Объекты интеллектуальной собственности, охраняемые патентным правом	12

Модуль 13
Обеспечение безопасности персональных данных

Код Темы	Наименование темы	Для включения в учебно - тематический план (объем часов)
13.1.	Общий порядок действий оператора по выполнению требований Федерального закона «О персональных данных»	8
13.2.	Этапы реализации требований Федерального закона «О персональных данных»	8
13.3.	Определение необходимости уведомления уполномоченного органа по защите персональных данных о намерении обработки персональных данных	8
13.4.	Классификация информационных систем обработки персональных данных	8
13.5.	Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных	8

Код Темы	Наименование темы	Для включения в учебно - тематический план (объем часов)
13.6.	Проектирование и реализация системы защиты персональных данных	8
13.7.	Организационные и технические меры защиты информации в информационных системах персональных данных	8
13.8.	Организация контроля защищенности персональных данных	8
13.9.	Типовое положение о разрешительной системе допуска к информационным ресурсам организации, содержащим персональные данные	8
13.10.	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	20
13.11.	Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	6

Модуль 14
Безопасность вычислительных сетей

Код Темы	Наименование темы	Для включения в учебно - тематический план (объем часов)
14.1.	Идентификация, аутентификация и управление доступом	4
14.2.	Криптографическая защита информации	4
14.3.	Сети периметра и стратегия удаленного доступа	4
14.4.	Технологии межсетевых экранов	4
14.5.	Протокол IPSec	4
14.6.	Виртуальные частные сети	4

Модуль 15
Защита информации в базах данных

Код Темы	Наименование темы	Для включения в учебно - тематический план (объем часов)
15.1.	Теоретические основы построения реляционных баз данных	4
15.2.	Клиент-серверная архитектура современных реляционных систем управления базами данных (СУБД)	4
15.3.	Теоретические основы безопасности баз данных и СУБД	4
15.4.	Механизмы и методы обеспечения целостности информации в реляционных базах данных	4
15.5.	Механизмы и методы обеспечения конфиденциальности информации в реляционных базах данных	4
15.6.	Механизмы и методы обеспечения доступности информации в реляционных базах данных	4
15.7.	Верификация баз данных и проведение аудита в СУБД	4

Модуль 16
Управление информационной безопасностью

Код Темы	Наименование темы	Для включения в учебно - тематический план (объем часов)
16.1.	Понятие системы управления информационной безопасностью (СУИБ)	4
16.2.	Стандартизация СУИБ	8
16.3.	Функциональные составляющие СУИБ	4
16.4.	Методологические основы управления информационными рисками	8
16.5	Нормативно-технические основы управления информационными рисками	8
16.6.	Инструментальные средства анализа информационных рисков	4

Модуль 17
Экономика защиты информации

Код Темы	Наименование темы	Для включения в учебно - тематический план (объем часов)
17.1.	Рынок информации: особенности и проблемы развития	8
17.2.	Правовые аспекты взаимодействия субъектов на рынке информации	8
17.3.	Основные принципы и методы защиты информации	4
17.4.	Интеллектуальная собственность предприятия и предпринимательский риск	4
17.5.	Сущность себестоимости продукции	4
17.6.	Принципы ценообразования	4
17.7.	Экономическая эффективность защиты информации	8

Модуль 18
Организация и управление службой защиты информации

Код Темы	Наименование темы	Для включения в учебно - тематический план (объем часов)
18.1.	Предпосылки создания подразделения по защите информации на предприятии	4
18.2.	Цели обеспечения информационной безопасности предприятия	4
18.3.	Место и роль службы защиты информации в организационной структуре предприятия	4
18.4.	Структура, формы и методы защиты информации на предприятии	8
18.5.	Структура и штат службы защиты информации	4
18.6.	Внутренние организационно-распорядительные документы службы подразделения по защите информации	8
18.7.	Виды, формы и порядок проведения контроля защищенности информации	8

Модуль 19
Комплексные системы защиты информации

Код Темы	Наименование темы	Для включения в учебно - тематический план (объем часов)
19.1.	Комплексная система защиты и место в ней комплексной системы защиты информации (КСЗИ)	8
19.2.	Управление процессами функционирования КСЗИ	12
19.3.	Принципы комплексной защиты корпоративной информации	8
19.4	Подсистемы информационной безопасности корпоративных информационных систем	8
19.5.	Нормативно-методическая составляющая КСЗИ	8
19.6.	Организационная составляющая КСЗИ	8
19.7.	Программно-аппаратная составляющая КСЗИ	8
19.8.	Инженерно-техническая составляющая КСЗИ	8

Модуль 20
Криптографическая защита информации

Код Темы	Наименование темы	Для включения в учебно - тематический план (объем часов)
20.1.	Место криптографии в системе научных знаний	8
20.2.	Симметричные криптосистемы. Шифры подстановок и перестановок	8
20.3.	Поточные шифры	8
20.4.	Блочные шифры	8
20.5.	Подтверждение целостности информации криптографическими средствами	8
20.6.	Подтверждение подлинности источника информации криптографическими средствами	8
20.7.	Управление ключами	8
20.8.	Порядок лицензирования деятельности по разработке,	12

Код Темы	Наименование темы	Для включения в учебно - тематиче-ский план (объем часов)
	производству, распространению шифровальных (крипто-графических) средств	

4.3 Перечень практических занятий (семинаров)

Код темы	Наименование практического занятия (семинара)	Кол-во часов
1.6.	Применение методик выявления угроз безопасности информации на объектах информатизации	2
1.8.	Разработка политики безопасности	16
4.6.	Применение методики организации и проведения лицензирования деятельности по осуществлению мероприятий по оказанию услуг в области технической защиты информации	10
4.7.	Изучение нормативных правовых документов по организации технической защиты информации ограниченного доступа	8
5.2.	Разработка пакета основных правил, инструкций, требований по обеспечению безопасности предприятия	10
5.5.	Подготовка и составление Положения о подразделении по защите информации	8
6.1.	Изучение основных видов документов	18
7.5.	Применение средств технической защиты информации	10
7.11.	Применение средств контроля состояния технической защиты информации на объектах информатизации	8
8.5.	Применение средств защиты от вредоносных программ	6
8.9.	Применение средств защиты информации от несанкционированного доступа	12
11.2.	Организация конфиденциального делопроизводства	6
11.6.	Обработка изданных конфиденциальных документов, систематизация документов	4
11.7.	Проверки наличия конфиденциальных документов, уничтожение носителей конфиденциальной информации, режим хранения	4
11.8.	Защита конфиденциальной информации в системе электронного документооборота	4
12.4.	Изучение нормативных правовых документов в области авторского права	6
12.5.	Изучение нормативных правовых документов в области смежного права	6
12.6.	Изучение нормативных правовых документов в области патентного права	6
13.4.	Классификация информационных систем обработки персональных данных	8
13.5	Выявление угроз безопасности персональных данных при их обработке в информационных системах персональных данных	4
13.7.	Определение организационных и технических меры защиты информации в информационных системах персональных данных	2
13.11.	Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	4
16.2.	Изучение стандартов систем управления информационной безопасностью	6
17.7.	Оценка экономической эффективности защиты информации	6
18.6.	Разработка внутренних организационно-распорядительные документы службы подразделения по защите информации	6

Код темы	Наименование практического занятия (семинара)	Кол-во часов
19.5.	Разработка нормативно-методической составляющей комплексной системы защиты информации	6
19.6.	Разработка организационной составляющей комплексной системы защиты информации	4
19.7.	Разработка программно-аппаратной составляющей комплексной системы защиты информации	4
19.8.	Разработка инженерно-технической составляющей комплексной системы защиты информации	4
20.4.	Изучение блочных алгоритмов шифрования	10
20.6.	Изучение асимметричных криптографических алгоритмов	8

4.4 Перечень тем курсовых работ

Код модуля	Тема курсовой работы
1.	Разработка политики безопасности предприятия (*на примере своего предприятия, организации учреждения*)
4.	Правовое регулирование деятельности по защите информации (*одна из категорий защищаемой информации*)
5.	Организационные мероприятия по обеспечению безопасности персональных данных (*на примере своего предприятия, организации учреждения*)
6.	Разработка комплекта документов предприятия (*на примере своего предприятия, организации учреждения*)
7.	Организация инженерно-технической защиты объекта (*на примере своего предприятия, организации учреждения*)
8.	Организация программно-аппаратной защиты информации (*на примере своего предприятия, организации учреждения*)
11.	Разработка комплекта конфиденциальных документов предприятия (*на примере своего предприятия, организации учреждения*)
12.	Анализ методов защиты интеллектуальной собственности (*одна из отраслей права*)
13.	Мероприятия по применению требований Постановлени Правительства РФ №1119 от 01.11.2012 во вновь создаваемых ИСПДн
19.	Анализ международных стандартов информационной безопасности (*на примере одного стандарта*)
20.	Применение методов симметричной и асимметричной криптографии к решению практических задач

5 Организационно-педагогические условия

Реализация рабочей программы ПК (ПП) проходит в полном соответствии с требованиями законодательства Российской Федерации в области образования, нормативными правовыми актами, регламентирующими данные направления деятельности (Приложение Г).

При обучении применяются различные виды занятий — лекции, практические занятия, лабораторные работы, экскурсии и т.д. При этом используются технические средства, способствующие лучшему теоретическому и практическому усвоению программного материала: видеофильмы, компьютеры, мультимедийные программы.

Для закрепления изучаемого материала проводится промежуточное тестирование, а также практические занятия на специальном оборудовании. Основные методические материалы размещаются на электронном носителе для последующей выдачи слушателям.

5.1 Организационные условия

Для обучения слушателей системы дополнительного профессионального образования университет располагает отдельным зданием ИДПО (Одинарка 1А).

При реализации программ используется учебно-производственная база университета, которая оснащена самым современным оборудованием и новейшими техническими средствами обучения.

Кроме того, что слушатели ИДПО в процессе обучения обеспечиваются необходимой нормативно-справочной и учебно-методической литературой, информационными материалами, они имеют возможность пользоваться научно-технической библиотекой, имеющей три читальных зала с книжным фондом более 600 тысяч экземпляров.

Желающие в свободное от учебы время могут под руководством опытных тренеров заниматься в спортивным комплексом университета.

Социальная инфраструктура жизнеобеспечения слушателей включает в себя общежитие гостиничного типа на 109 номеров (35 трехместных, 62 двухместных и 12 одноместных), комбинат общественного питания с сетью столовых и кафе.

Главный учебный корпус университета, здание ИДПО, общежитие слушателей, комбинат общественного питания расположены в живописном месте г. Екатеринбурга (т.н. «генеральские дачи») в непосредственной близости друг от друга.

Каждую неделю в свободное от учебы время для слушателей проводится экскурсия либо по г. Екатеринбургу, либо на Ганину яму (место захоронения последнего Российского императора).

5.2 Педагогические условия

Занятия в ИДПО ведут высококвалифицированные преподаватели УрГУПС и других ВУЗов города, руководители и специалисты ОАО «РЖД», научные работники Уральского отделения ВНИИЖТ, специалисты и опытные практические работники ведущих промышленных предприятий и научных учреждений.

5.3 Материально–техническое обеспечение

Здание ИДПО содержит 20 учебных аудиторий общей площадью 1000 м^2. Из них шесть компьютерных класса, всего 81 компьютеров. Все аудитории оборудованы видеопроекторами и мультимедийными средствами.

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
Аудитория	лекции	Компьютер, мультимедийный проектор, экран, доска
Лаборатория	практические занятия	- Комплекс виброакустических измерений «СПРУТ-7А». - Универсальный анализатор проводных коммуникаций (пятое поколение) «Улан-2». - Автоматизированная система измерения действующих высот случайных антенн и коэффициентов реального затухания электромагнитных сигналов «СТЕНТОР». - Анализатор спектра R&S FSH 4/8.
Компьютерный класс	практические занятия	- Система защиты информации на серверах и рабочих станциях от несанкционированного доступа SecretNet 5.0. - Программный комплекс «ViPNet Custom 3.0». - Аппаратно-программный комплекс шифрования «Континент» версия 3.0

6 Формы аттестации

- Промежуточное тестирование;
- Итоговое тестирование;
- Комиссионная защита выпускных работ;

7. Оценочные материалы

7.1.Оценка качества освоения программы

По программам повышения квалификации оценка качества освоения программы осуществляется на основе итогового тестирования по пятибалльной системе оценок.

Слушатель получает оценку 5, если он дает правильные ответы на 80-100% предложенных вопросов.
Слушатель получает оценку 4, если он дает правильные ответы на 60-79% предложенных вопросов.
Слушатель получает оценку 3, если он дает правильные ответы на 40-59% предложенных вопросов.
Слушатель получает оценку 2, если он дает правильные ответы на 0-39% предложенных вопросов.

Слушатель считается аттестованным, если он получил положительную оценку (3,4 или 5).

По программам профессиональной переподготовки оценка качества освоения программы осуществляется на основе:

1. Промежуточного тестирования по темам каждого модуля, входящего в программу на основе пятибалльной системы оценок по указанным выше критериям.

2. Защиты курсовых работ на основе пятибалльной системы оценок.

Оценка по результатам защиты курсовой работы может быть снижена:
- за ошибки в формальных выкладках и численных расчетах, неверное графическое отображение и ошибочную интерпретацию полученных результатов;
- неправильные ответы при защите на вопросы по теоретической и практической части работы;
- наличие грубых и явных орфографических и синтаксических ошибок;

- несоответствие требованиям оформления текстовой и графической частей.

Курсовая работа не допускается к защите и считается невыполненной:

- за несоответствие проделанной работы выданному заданию;
- за нарушения, выявленные при проверке на плагиат, характер которых ставит под сомнение самостоятельность выполнения в объеме не менее 70% от общего объема курсовой работы.

3. Комиссионной защиты выпускной работы на основе пятибалльной системы оценок.

Оценка по результатам защиты выпускной работы может быть снижена:

- за ошибки в формальных выкладках и численных расчетах, неверное графическое отображение и ошибочную интерпретацию полученных результатов;
- неправильные ответы при защите на вопросы по теоретической и практической части работы;
- наличие грубых и явных орфографических и синтаксических ошибок;
- несоответствие требованиям оформления текстовой и графической частей.

Выпускная работа не допускается к защите и считается невыполненной:

- за несоответствие проделанной работы выданному заданию;
- за нарушения, выявленные при проверке на плагиат, характер которых ставит под сомнение самостоятельность выполнения в объеме не менее 70% от общего объема выпускной работы.

Решение об оценке защиты выпускной работы принимается на закрытом заседании государственной аттестационной комиссии (ГАК) путем голосования и оформляется протоколом заседания. Результаты защиты оглашаются председателем ГАК публично в присутствии слушателей в тот же день, когда ими были защищены выпускные работы.

Слушатель считается аттестованным, если по всем формам аттестации он получил положительную оценку (3,4 или 5).

Список использованной литературы

Основная литература

1. Конституция Российской Федерации от 25 декабря 1993 года, с изменениями от 30 декабря 2008 г. N 6-ФКЗ и от 30 декабря 2008 г. N 7-ФКЗ).
2. Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ.
3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ (в ред. от 21 июля 2011 г. № 252-ФЗ).
4. Федеральный закон «О государственной тайне» от 21 июля 1993 года № 5485-I (в ред. от 08.11.2011 N 309-ФЗ.
5. Федеральный закон «О коммерческой тайне » от 18.12.2006 №231-ФЗ.
6. Федеральный закон «О лицензировании отдельных видов деятельности» от мая 2011 года N 99-ФЗ (в ред. от 28.07.2012г. №133-ФЗ).
7. Федеральный закон «О персональных данных » от 27 июля 2006 г. № 149-ФЗ.
8. Доктрина информационной безопасности Российской Федерации (Утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895).
9. Постановление Правительства Российской Федерации «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне от 06 февраля 2010г. № 63.
10. Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» (в ред. от 31.03.2010 № 200, от 24.09.2010 № 749).
11. Постановление Правительства Российской Федерации от 1 ноября 2012г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
12. Постановление Правительства Российской Федерации от 26.06.1995 №608 (ред. от 21.04.2010 г.) «О сертификации средств защиты информации».
13. Постановление Правительства Российской Федерации от 29 декабря 2007г. №957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами».

14. Постановление Правительства Российской Федерации от 17 ноября 2007г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

15. Постановление Правительства Российской Федерации от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

16. Указ Президента Российской Федерации от 6 марта 1997 года № 188 (в ред. от 23.09.2005 №1111) «Об утверждении Перечня сведений конфиденциального характера».

17. Методический документ «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при обработке в информационных системах персональных данных». Утвержден руководством 8 Центра ФСБ России 21 февраля 2008г. №149/6/6-622.

18. Методический документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008г.

19. Методический документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 14 февраля 2008г.

20. Приказ Россвязькомнадзора от 17 июля 2008г. № 8 «Об утверждении образца формы уведомления об обработке персональных данных».

21. Приказ Россвязькомнадзора от 18 февраля 2009г. №42 «О внесении изменений в приказ Россвязькомнадзора от 17 июля 2008г. № 8 «Об утверждении образца формы уведомления об обработке персональных данных».

22. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

23. Руководящий документ Гостехкомиссии Российской Федерации «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации».

24. Руководящий документ Гостехкомиссии Российской Федерации «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

25. Руководящий документ Гостехкомиссии Российской Федерации «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации».

26. ГОСТ Р 50922-96 «Защита информации. Основные термины и определения».

27. ГОСТ 34.601-89 «Информационная технология. Стадии создания автоматизированных систем».

28. ГОСТ Р 34.602-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

29. ГОСТ Р ИСО/МЭК 27000-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».

30. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

31. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»

32. ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»

33. ГОСТ Р ИСО/МЭК 27003-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности»

34. Аграновский, А.В. Практическая криптография: алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади. М.: Изд-во «Солон-Пресс, 2009. – 256 с.

35. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др. – М.: Горячая Линия - Телеком, 2012. – 497 с.

36. Грибунин, В.Г. Комплексная система защиты информации на предприятии / В.Г. Грибунин. – М.: Издательский центр «Академия», 2009. - 416 с.

37. Домарев, В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. – К.: ООО «ТИД ДС», 2008.

38. Зайцев, А.П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещаряков и др. - М.:ООО «Издательство Машиностроение», 2009 -508 с.

39. Кокшаров, В.А. Экономика организаций. Учебно-методическое пособие / В.А. Кокшаров. – Екатеринбург: Изд-во УрГУПС, 2011. – 63 с.

40. Куняев, Н.Н. Конфиденциальное делопроизводство и защищенный электронный документооборот / Н.Н. Куняев, А.С. Дёмушкин, Т.В. Кон-

драшова, А.Г. Фабричнов; под общ. ред. Н.Н. Куняева. Учебник - М.: Логос, 2011г.

41. Мухин, В.И. Управление интеллектуальной собственностью (учеб.для студентов вузов) / В.И. Мухин. - М.: Гуманитар. изд. центр ВЛАДОС, 2008. - 335с.

42. Орин, Т. Администрирование корпоративных сетей на основе Windows Server 2008 / Т. Орин, Д. Поличелли, Й. Маклин, Дж. К. Макин, П. Менкьюзо, Д.Р. Миллер. – М.: Русская редакция, 2011. – 504 с.

43. Паршина, Е.В. Проектирование информационных систем. Конспект лекций / Е.В. Паршина, К.А. Паршин. – Изд-во УрГУПС, 2010.

44. Платонов, В.В. Программно-аппаратные средства защиты информации / В.В. Платонов. – М.: Академия, 2013. – 396 с.

45. Смагин, А.А. Базовые принципы информационной безопасности вычислительных систем / А.А. Смагин. – Ульяновск.: Ульяновский государственный технический университет, 2009. – 168 с.

46. Таненбаум, Э. Компьютерные сети / Э. Таненбаум. – Санкт-Петербург: Питер, 2011. – 991с.

47. Торокин, А.А. Инженерно-техническая защита информации (учеб.пособие для студентов, обучающихся по специальностям в обл. информ.безопасности) / А.А. Торокин.- М.: Изд-о Гелиос АРВ, 2008.-960 с.

48. Черемушкин, А.В. Криптографические протоколы. Основные свойства и уязвимости / А.В. Черемушкин. М.: Академия, 2009. – 272 с.

49. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.

50. Шепитько, Г.Е. Экономика защиты информации / Г.Е. Шепитько. – Изд-во «Москва», 2011. – 64 с.

Дополнительная литература

1. Гражданский Кодекс РФ: часть 1 от 30.11.1994 N 51-ФЗ (ред. от 30.11.2011); часть 2 от 26.01.1996 N 14-ФЗ (ред. от 30.11.2011); часть 3 от 26.11.2001 N 146-ФЗ (ред. от 30.06.2008); часть 4 от 18.12.2006 N 230-ФЗ (ред. от 08.12.2011).

2. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 года № 195-ФЗ (в ред. от 6 декабря 2011 г. N 404-ФЗ).

3. Уголовный кодекс Российской Федерации от 24 мая 1996 г. № 63-ФЗ (в ред. от 07.12.2011 N 420-ФЗ).

4. Федеральный закон «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» от 21 июля 1997г. №119-ФЗ.

5. Федеральный закон «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию» от 15 августа 1996 г. № 114-ФЗ (в ред. от 6 декабря 2011 г. N 397-ФЗ).

6. Федеральный закон «О техническом регулировании» от 27.12.2002 №184-ФЗ (в ред. от 28.07.2012).

7. Федеральный закон «О Федеральной службе безопасности» от 3 апреля 1995 г. № 40-ФЗ (в ред. от 27 июля 2010 г. N 238-ФЗ).

8. Положение о межведомственной комиссии по защите государственной тайны (в ред. Указов Президента РФ от 26.02.2009 N 228, от 14.02.2012 N 183).

9. Положение о сертификации средств защиты информации по требованиям безопасности информации (утв. Приказом Гостехкомиссии РФ от 27.10.1995г. №199).

10.Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. Гостехкомиссией РФ 25.11.1994 г.).

11.Постановление Правительства РФ от 3 ноября 1994г.№1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

12.Приказ ФСБ РФ от 13.11.1999 N 564 «Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия» (Зарегистрировано в Минюсте РФ 27.12.1999г. №2028).

13.Приказ Министерства культуры и массовых коммуникаций Российской Федерации от 8 ноября 2005г. № 536 «О Типовой инструкции по делопроизводству в федеральных органах исполнительной власти».

14.Указ Президента Российской Федерации «Вопросы Федеральной службы по техническому и экспортному контролю» от 16 августа 2004 года № 1085 (в ред. от 23.10.2008г. №1517).

15.Руководящий документ Гостехкомиссии Российской Федерации «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».

16.ГОСТ Р 6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов».

17.ГОСТ Р 51141-98 «Делопроизводство и архивное дело. Термины и определения».

18.ГОСТ 34.603 - 92 «Информационная технология виды испытаний автоматизированных систем».

19.ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

20.Приказ ОАО «РЖД» от 27 декабря 2004г. №240 «О порядке обращения с информацией, составляющей коммерческую тайну, в ОАО «РЖД» (в ред. Приказа ОАО «РЖД» от 19.11.2006 №267).

21.Грабер, М. Введение в SQL / М. Грабер. – М.:Лори, 2010. – 228 с.

22.Гугуева, Т.А. Конфиденциальное делопроизводство: Учебное пособие / Т.А. Гугуева. – М.: Изд.: Альфа-М, 2012г.

23.Диго, С.М. Базы данных. Проектирование и создание / С.М. Диго. - М:. Изд. центр ЕАОИ, 2008. – 172 с.

24.Загинайлов, Ю.Н. Комплексная система защиты информации на предприятии. Учебно-методическое пособие / Ю.Н. Загинайлов и др. - Барнаул: АлтГТУ, 2010. – 287 с.

25.Кришталюк, А.Н. Конфиденциальное делопроизводство и защита коммерческой тайны. Учебно-методическое пособие / А.Н. Кришталюк. - г. Орел, 2011г.

26.Кудрявцев, К.Я. Создание баз данных / К.Я. Кудрявцев. – М.: НИЯУ МИФИ, 2010. – 155 с.

27.Кузин, А.В. Базы данных / А.В. Кузин, С.В. Левонисова. – М.: Академия, 2008.

28.Панасенко, С. Алгоритмы шифрования. Специальный справочник / С. Панасенко. Спб: БХВ-Петербург, 2009.

29.Токмаков, Г.П. Базы данных. Концепция баз данных, реляционная модель данных, языки SQL и XML / Г.П. Токмаков. – УлГТУ, 2010. – 193 с.

30.Черенев, Ю.Б. Пожарно-охранная сигнализация: сб. лабораторных работ / Ю.Б. Черенев. - Екатеринбург: Изд-во УрГУПС, 2010. – 48 с.

31.Черенев, Ю.Б. Видеоохранные системы: практикум / Ю.Б. Черенев. – Екатеринбург: Изд-во УрГУПС, 2009. – 48 с.

Составители программы

1. Зырянова Т.Ю., канд. техн. наук (Раздел 1, 2, 3. Раздел 4 - темы 15.1-15.7, 16.1-16.6, 19.1-19.8, 20.8. Раздел 5, 6, 7, 8).

2. Гузенкова Е.А. (Раздел 4 – темы 8.1-8.9, 14.1-14.6).

3. Жайворонская О.Ю. (Раздел 4 – темы 10.1-10.6).

4. Каргапольцева М.Н. (Раздел 4 – темы 5.1-5.9).

5. Медведев Н.В., канд. техн. наук (Раздел 4 – темы 3.1-3.6, 20.1-20.7).

6. Паршин К.А., канд. техн. наук, доцент (Раздел 4 – темы 1.1.-1.8, 9.1-9.8).

7. Селина О.В. (Раздел 4 – темы 17.1-17.7).

8. Симонович В.Г. (Раздел 4 – темы 2.1-2.8, 13.1-13.11).

9. Черенев Ю.Б. (Раздел 4 – темы 7.1-7.11, 12.1-12.6, 18.1-18.7).

10. Чукалова Л.Г. (Раздел 4 – темы 6.1-6.7, 11.1-11.8).

Приложение А

Примерный перечень

рабочих программ повышения квалификации, составленных на основе модульной дополнительной профессиональной программы «Информационная безопасность»

№№ пп.	Наименование программ	Код тем	Категории слушателей	Продолжительность обучения
1	Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных	1.6 7.9 5.8 7.10 8.9 13.5 13.7 13.10 13.11	Специалисты органов государственной власти по защите информации, осуществляющие разработку и эксплуатацию автоматизированных информационных систем, обеспечивающих обработку, хранение и передачу персональных данных.	72 ч
2	Техническая защита информации	4.6 4.7 5.9 7.5 7.11 9.8	Руководители, главные специалисты, начальники подразделений защиты информации аппаратов органов государственной власти. Руководители, главные специалисты, начальники подразделений защиты информации предприятий (организаций, учреждений). Специалисты по защите информации (по технической защите информации). Специалисты по защите информации (по оценке и аудиту). Специалисты по защите информации (по лицензированию и сертификации). Руководители, инженерно-технические работники, научные работники научно-исследовательских инсти-	72 ч

№№ пп.	Наименование программ	Код тем	Категории слушателей	Продолжительность обучения
			тутов, конструкторских, изыскательских, проектных организаций.	

№№ пп.	Наименование программ	Код тем	Категории слушателей	Продолжительность обучения
3	Информационная безопасность	1.1 – 1.8 2.1 – 2.8 3.1 – 3.6 4.1 – 4.7 5.1 – 5.7 6.1 – 6.7 7.1 – 7.8 8.1 – 8.8 9.1 – 9.7 10.1 – 10.6 11.1- 11.8 12.1 – 12.6 13.1 – 13.6, 13.8 – 13.10 14.1 – 14.6 15.1 – 15.7 16.1 – 16.6 17.1 – 17.7 18.1 – 18.7 19.1 – 19.8 20.1 – 20.8	Руководители, главные специалисты, начальники подразделений защиты информации аппаратов органов государственной власти. Руководители, главные специалисты, начальники подразделений защиты информации предприятий (организаций, учреждений). Специалисты по защите информации (по технической защите информации). Специалисты по защите информации (по оценке и аудиту). Специалисты по защите информации (по лицензированию и сертификации). Руководители, инженерно-технические работники, научные работники научно-исследовательских институтов, конструкторских, изыскательских, проектных организаций.	504 ч

Приложение Б

СОГЛАСОВАНО:
Должность, предприятие

_____Ф.И.О.
«____» _____201 г.

УТВЕРЖДАЮ:
Директор АКО УрГУПС

_____И.Л. Васильев
«____» _____201 г.

Учебно–тематический план рабочей программы повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» в ИДПО АКО

Категория слушателей: специалисты органов государственной власти по защите информации, осуществляющие разработку и эксплуатацию автоматизированных информационных систем, обеспечивающих обработку, хранение и передачу персональных данных

Форма обучения: очная

Трудоемкость: 72 часа

Срок освоения: 10 дней очно

Режим занятий: 6 - 10 академических (45 мин.) часов в день, 36 часов аудиторной учебной и самостоятельной работы под руководством преподавателя в неделю.

№	Наименование тем	Всего часов	Обучение			Преподаватель
			очное		заочное с применением ДОТ	
			лекции	практика		
1	2	3	4	5	6	7
	Общие вопросы технической защиты информации	**22**	**16**	**6**		
	1. Правовые и организационные основы технической защиты информации ограниченного доступа	8	8			Чукалова Л.Г.
	2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	14	8	6		Черенев Ю.Б.

1	2	3	4	5	6	7
	Организация обеспечения безопасности персональных данных в информационных системах персональных данных	**46**	**36**	**10**		
	3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных.	20	14	6		Симонович В.Г.
	4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.	20	20			Симонович В.Г.
	5. Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	6	2	4		Симонович В.Г.
	Итого по видам занятий	**68**	**52**	**16**		
	Итоговая аттестация: итоговое тестирование	**4**				
	Всего	**72**	**52**	**16**		

Приложение В

Календарный учебный график

Очное									
Количество часов									
РД1	РД2	РД3	РД4	РД5	РД6	РД7	РД8	РД9	РД 10
6	8	8	8	8	8	8	8	6	4

Приложение Г

Нормативные документы по ДПО

№ п/п	Наименование	Ссылка
Федеральные законы		
1	Федеральный закон Российской Федерации от 29 декабря 2012 г. №273-ФЗ "Об образовании в Российской Федерации"	Читать
2	Сравнительный анализ Закона РФ от 10 июля 1992 г. №3266-I "Об образовании" и Федерального закона от 29 декабря 2012 г. №273-ФЗ "Об образовании в Российской Федерации" (подготовлен экспертами компании "Гарант")	Читать
3	Федеральный закон от 02 июля 2013 г. №185-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу законодательных актов (отдельных положений законодательных актов) Российской Федерации в связи с принятием Федерального закона "Об образовании в Российской Федерации"	Читать
Постановления Правительства РФ		
4	Постановление Правительства Российской Федерации от 10 июля 2013 г. №582 "Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети "Интернет" и обновления информации об образовательной организации"	Читать
5	Постановление Правительства РФ от 26 августа 2013 г. №729 О федеральной информационной системе "Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении"	Читать
6	Постановление Правительства РФ от 5 августа 2013 г. №662 "Об осуществлении мониторинга системы образования"	Читать
7	Постановление Правительства РФ от 30.03.2013 №286 «О формировании независимой системы оценки качества работы организаций, оказывающих социальные услуги»	Читать
8	Постановление Правительства РФ от 08.08.2013 №678 "Об утверждении номенклатуры должностей педагогических работников организаций, осуществляющих образовательную деятельность, должностей руководителей образовательных организаций"	Читать
9	Проект Постановления Правительства РФ «Об утверждении Положения о лицензировании образовательной деятельности (за исключением указанной деятельности, осуществляемой частными образовательными организациями, находящимися на территории инновационного центра «Сколково»)»	Читать
10	Проект Постановления Правительства РФ «Об утверждении Положения о государственной аккредитации образовательной деятельности»	Читать
11	Постановление Правительства Российской Федерации от 31 августа 2013 г. №755 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего	Читать

	образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования»	
12	Постановление Правительства Российской Федерации от 20 августа 2013 г. №719 «О государственной информационной системе государственного надзора в сфере образования»	Читать
13	Постановление Правительства Российской Федерации от 15 августа 2013 г. №706 «Об утверждении правил оказания платных образовательных услуг»	Читать
14	Постановление Правительства Российской Федерации от 05 августа 2013 г. №661 «Об утверждении правил разработки, утверждения федеральных государственных образовательных стандартов и внесения в них изменений»	Читать
15	Постановление Правительства Российской Федерации от 25 июля 2013 г. №627 «Об утверждении требований к осуществлению государственного контроля (надзора) в сфере образования за деятельностью образовательных организаций, реализующих образовательные программы, содержащие сведения, составляющие государственную тайну»	Читать
16	Постановление Правительства Российской Федерации от 20 июля 2013 г. №611 «Об утверждении правил подтверждения документов об образовании и (или) о квалификации»	Читать
17	Постановление Правительства Российской Федерации от 15 июля 2013 г. №594 «Об утверждении положения о Федеральной службе по надзору в сфере образования и науки»	Читать
18	Постановление Правительства Российской Федерации от 03 июня 2013 г. №466 «Об утверждении положения о Министерстве образования и науки Российской Федерации»	Читать
19	Постановление Правительства Российской Федерации от 24 мая 2013 г. №438 «О государственной информационной системе "Реестр организаций, осуществляющих образовательную деятельность по имеющим государственную аккредитацию образовательным программам"»	Читать
Приказы и письма Министерства образования и науки РФ		
20	Приказ Министерства образования и науки Российской Федерации от 1 июля 2013 г. №499 г. Москва "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам"	Читать
21	Приказ Министерства образования и науки Российской Федерации от 14 июня 2013 г. №462 г. Москва "Об утверждении Порядка проведения самообследования образовательной организацией"	Читать
22	Приказ Министерства образования и науки РФ «Об утверждении квалификационных требований к экспертам, требований к экспертным организациям, привлекаемым к проведению аккредитационной экспертизы»	Читать
23	Проект приказа Минобрнауки РФ «Об утверждении типовых положений об учебно-методических объединениях в системе образования»	Читать
24	Приказ Министерства образования и науки Российской Федерации от 23	Читать

25	Приказ Министерства образования и науки Российской Федерации от 18 апреля 2013 г. №292 «Об утверждении порядка организации и осуществления образовательной деятельности по основным программам профессионального обучения»	Читать
26	Письмо Министерства образования и науки Российской Федерации от 09 июля 2013 г. №ДЛ-187/17 «В дополнение к разъяснениям о наименовании образовательных учреждений»	Читать
27	Письмо Министерства образования и науки Российской Федерации от 10 июня 2013 г. №ДЛ-151/17 «О наименовании образовательных учреждений»	Читать
28	Письмо Минобрнауки России от 01 апреля 2013 г. №ИР-170/17 «О Федеральном законе "Об образовании в Российской Федерации"»	Читать
29	Письмо заместителя Министра образования и науки РФ А.А. Климова «О документах о квалификации» от 02.09.2013 №АК-1879/06	Читать
30	Приказ «О комиссии Министерства образования и науки Российской Федерации по развитию дополнительного профессионального образования»	Читать
31	Письмо Министерства образования и науки РФ от 22 июля 2013 г. № 09-889 «О размещении на официальном сайте информации»	Читать
Приказы Министерства труда и социальной защиты РФ		
32	Приказ Министерства труда и социальной защиты РФ от 12.04.2013 №148н «Об утверждении уровней квалификации в целях разработки проектов профессиональных стандартов»	Читать
33	Приказ Министерства труда и социальной защиты РФ от 12.04.2013 №147н «Об утверждении Макета профессионального стандарта»	Читать
34	Проект приказа Министерства труда и социальной защиты РФ от 14 февраля 2013 г. «Об утверждении уровней квалификации в целях подготовки профессиональных стандартов»	Читать

Заместитель директора АКО по дополнительному профессиональному образованию: А.Н. Штин

Заведующая Учебно- методическим отделом АКО В.Л. Леванова

Старший преподаватель – организатор Учебного центра дистанционных и компьютерных технологий Л.М.Пичугина