МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЛИПЕЦКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ П.П. СЕМЕНОВА-ТЯН-ШАНСКОГО»

УТВЕРЖДАЮ
И.о. ректора ФГБОУ ВО «ЛГПУ»
_____ Н.В. Федина
«16» апреля 20 17 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
курсов повышения квалификации

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Разработчик программы:
Институт естественных, математических и технических наук
кафедра информатики, информационных технологий и защиты информации

Липецк – 2017

1. Структура программы повышения квалификации

1.1. Общая характеристика дополнительной образовательной программы:

1.1.1. Законодательные и нормативные правовые акты, в соответствии с которыми разрабатывалась программа повышения квалификации:

Федеральный закон от 09.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

приказ Минобрнауки России от 01.07.2013 № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» (зарегистрирован в Минюсте России 20.08.2013 № 29444);

Единый квалификационный справочник должностей руководителей, специалистов и служащих, раздел «Квалификационные характеристики должностей работников образования», утвержденный приказом Минздравсоцразвития России от 26.08.2010 № 761н (зарегистрирован в Минюсте России 06.10.2010 № 18638), в ред. приказа Минздравсоцразвития России от 31.05.2011 N 448н;

приказ Минтруда России от 13.10.2014 N 716н "Об утверждении профессионального стандарта "Менеджер по информационным технологиям" (Зарегистрировано в Минюсте России 14.11.2014 N 34714);

письмо Минобрнауки России от 02.09.2013 № АК-1879/06 «О документах о квалификации».

1.1.2. Тип дополнительной профессиональной программы: программа повышения квалификации (далее – программа).

1.1.3. Программа направлена на совершенствование компетенций, необходимых для профессиональной деятельности и повышение профессионального уровня в рамках имеющейся квалификации.

1.1.4. К освоению программы допускаются: лица, имеющие высшее, среднее профессиональное, начальное профессиональное или среднее (полное) общее образование; лица, получающие высшее профессиональное, среднее профессиональное или начальное профессиональное образование.

1.1.5. Срок освоения программы: 36 часов.

1.1.6. Форма обучения: очная, курсовая, дневная.

1.1.7. Категория обучающихся:

муниципальные служащие.

1.1.8. Формы аттестации обучающихся: итоговая аттестация в форме зачета.

1.1.9. Документ о квалификации: лицам, успешно освоившим программу и прошедшим итоговую аттестацию, имеющие высшее или среднее специальное образование выдается удостоверение о повышении квалификации установленного ФГБОУ ВО «ЛГПУ имени П.П. Семенова-Тян-Шанского» образца, иным слушателям сертификат об обучении.

Удостоверение о повышении квалификации дает право заниматься определенной профессиональной деятельностью и выполнять конкретные трудовые функции, для которых определены обязательные требования к наличию квалификации по результатам дополнительного профессионального образования.

1.1.10. При освоении программы параллельно с получением высшего профессионального или среднего профессионального образования удостоверение о повышении квалификации выдается одновременно с получением соответствующего документа об образовании.

1.2. Цели обучения:

Совершенствование компетенций, необходимых для профессиональной деятельности и повышения профессионального уровня в рамках имеющейся квалификации:

а) общекультурные компетенции (ОК):

- способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);

б) общепрофессиональные компетенции (ОПК):

- способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4);
- способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);

в) профессиональные компетенции (ПК):

- способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);
- способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);
- способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3);
- способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4).

1.3. Планируемые результаты обучения:

В результате освоения программы слушатель должен приобрести следующие знания и умения, необходимые для качественного изменения компетенций, указанных в разделе:

Слушатель должен знать:

- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
- аппаратные средства вычислительной техники;
- операционные системы персональных ЭВМ;
- структуру систем документационного обеспечения;
- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы

Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

- правовые основы организации защиты конфиденциальной информации;
- принципы и методы организационной защиты информации;
- технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;
- принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы, протекающие в них.

Слушатель должен уметь:

- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- анализировать и оценивать угрозы информационной безопасности объекта;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- пользоваться нормативными документами по защите информации.

Слушатель должен владеть:

- методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений;
- навыками выявления и уничтожения компьютерных вирусов;
- навыками работы с нормативными правовыми актами;
- методами технической защиты информации;
- методами формирования требований по защите информации;
- профессиональной терминологией.

В результате совершенствования указанных компетенций слушатель получает возможность реализовать в своей профессиональной деятельности, следующие трудовые функции:

- Установка программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД (A/01.5);
- Анализ угроз информационной безопасности в сетях электросвязи (D/01.7);
- Управление рисками систем защиты сетей электросвязи от НСД (F/01.7).

Соотношение между целями обучения и планируемыми результатами обучения может быть представлено в виде таблицы:

№ п/п	Совершенствуемые профессиональные компетенции	Уровень трудовой функции (отметить ячейку)			Соответствие компетенции направлению и уровню подготовки	Код трудовой функции
		знание	умение	владение		
1	2	3	4	5	6	7
1	способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4)	+	+	+	+	D/01.7
2	способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4)		+	+	+	D/01.7
3	способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)		+	+	+	D/01.7
4	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)	+	+	+	+	A/01.5
5	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)	+	+	+	+	A/01.5
6	способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3)	+	+	+	+	A/01.5
7	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)	+	+	+	+	F/01.7

1.4. Требования к уровню подготовки поступающего на обучение, необходимому для освоения программы.

Лица, желающие освоить дополнительную профессиональную программу, должны иметь:

высшее, среднее профессиональное, начальное профессиональное или среднее (полное) общее образование;

лица, получающие высшее профессиональное, среднее профессиональное или начальное профессиональное образование.

1.5. Учебный план

№	Наименование разделов и дисциплин	Всего часов	В том числе, час	
			Л	ЛР
1	Правовая защита информации	8	8	0
2.	Организационная защита информации	8	8	0
3.	Инженерно-техническая защита информации	10	2	8
4.	Защита информации в компьютерных системах	8	2	6
5.	Итоговый зачет	2		
	Всего часов	**36**	**20**	**14**

Примечание: Л – лекции, ЛР – лабораторная работа

2. Организационно-педагогические условия реализации программы

2.1. Материально-технические условия реализации программы.

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
Аудитория	лекции	компьютер, мультимедийный проектор, экран, доска
Компьютерный класс	лабораторные занятия	компьютеры, доска, офисное программное обеспечение
Лаборатория по защите информации	лабораторные занятия	компьютеры, доска, специализированное оборудование по защите информации

2.2. Форма организации образовательной деятельности.

2.2.1. Программа состоит из 4-х дисциплин, достаточных для формирования необходимых компетенций для ведения деятельности в области информационной безопасности. Дисциплины включают в себя перечень, трудоемкость, последовательность и распределение учебных часов, иных видов учебной деятельности обучающихся.

2.3. Условия реализация программы:

2.3.1. Обучение по программе осуществляется на основе договора об образовании, заключаемого со слушателем и (или) с физическим или юридическим лицом, обязующимся оплатить обучение лица, зачисляемого на обучение.

2.3.2. Обучение осуществляется единовременно и непрерывно.

2.3.3. Местом обучения является место нахождения ФГБОУ ВО «ЛГПУ имени П.П. Семенова-Тян-Шанского».

2.4. Ресурсы для реализации программы:

Профессиональный штат педагогических работников, создающих комплекс учебно-методических материалов и реализующих учебный процесс.

2.5. Иные условия реализация программы:

2.5.1. Возможно обучение по индивидуальному учебному плану в пределах осваиваемой программы в порядке, установленном локальными нормативными актами ФГБОУ ВО «ЛГПУ имени П.П. Семенова-Тян-Шанского».

2.5.2. Образовательный процесс осуществляется в течение всего календарного года.

2.5.3. Программа может реализовываться как самостоятельно ФГБОУ ВО «ЛГПУ имени П.П. Семенова-Тян-Шанского», так и посредством сетевых форм реализации.

3. Рабочие программы дисциплин

3.1. Правовая защита информации

3.1.1. Цели и задачи:

формирование правовой грамотности, понятия персональных данных, особенности защиты персональных данных, взаимосвязь нормативно-правового обеспечения защиты персональных данных с другими направлениями в области информационной безопасности;

3.1.2. Тематическое содержание дисциплины

№	Наименование тем	Всего часов
1.1	История развития законодательства в области защиты персональных данных в России и за её пределами	2 (Л)
1.2	Нормативно-правовое обеспечение защиты персональных данных	2 (Л)
1.3	Ответственность за нарушение законодательства России в сфере защиты персональных данных	4 (Л)
Итого		8 (Л)

Примечание: Л – лекции

Методические указания для обучающихся по освоению дисциплины (содержание дисциплины)

Тема № 1 История развития законодательства в области защиты персональных данных в России и за её пределами

Введение. Предмет и задачи курса. Значение и место курса в подготовке специалистов в области информационных систем и технологий. Структура курса. Разделы и темы, их распределение по видам аудиторных занятий. Состав и методы самостоятельной работы студентов по изучению дисциплины. Формы проверки знаний. Анализ нормативных источников, научной и учебной литературы.

История развития законодательства в области защиты персональных данных на территории России

История развития законодательства в области защиты персональных данных на территории США

История развития законодательства в области защиты персональных данных на территории Евросоюза.

Тема № 2 Нормативно-правовое обеспечение защиты персональных данных

Основные определения в области обработки персональных данных. Принципы и условия обработки персональных данных. Основные права субъекта персональных данных. Обязанности оператора персональных данных связанные с их хранением и обработкой. Документы ФСТЭК и уровень охраны соответствующей информации составляющей персональные данные. Биометрические персональные данные и особенности работы с ними. Надзорные органы в области регулирования информационных процессов, связанных с обработкой персональных данных и их полномочия.

Тема № 3 Ответственность за нарушение законодательства России в сфере защиты персональных данных

Ответственность оператора за безопасность информации содержащей персональные данные. Ответственность должностных лиц за нарушение правил работы с персональными данными. Ответственность физических лиц за неправомерный сбор, хранение и использование персональных данных.

3.1.3. Требования к уровню освоения содержания дисциплины

В результате освоения блока слушатель должен:

Знать: основные понятия, используемые при работе с персональными данными; основные права субъекта персональных данных; обязанности оператора персональных данных связанные с их хранением и обработкой; ответственность за нарушение законодательства Росси в области защиты информации.

Уметь: обращаться с документами, содержащими персональные данные; составлять договора на право обработки персональных данных; запрашивать документы, содержащие персональные данные субъекта в государственных органах.

Владеть: принципами и условиями обработки персональных данных.

3.2. Организационная защита информации

3.2.1. Цели и задачи:

сформировать принципы, силы, средства и условия организационной защиты информации на предприятии; рассмотреть организацию аналитической работы по предупреждению утечки конфиденциальной информации; направления и методы работы с персоналом, обладающим конфиденциальной информацией.

3.2.2. Тематическое содержание дисциплины

№	Наименование тем	Всего часов
1	Понятие «организационная защита информации»	2 (Л)
2	Аналитическая работа как основа управления системой организационной защиты информации	2 (Л)
3	Планирование процессов организационной защиты информации	4 (Л)
Итого		8 (Л)

Примечание: Л – лекции

Тема 1. Понятие «организационная защита информации»

Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими. Организационные методы как реализация полномочий и их распределение между уровнями управления организацией.

Понятия "организационная защита информации" и "режим защиты информации". Различные подходы к определению понятия "организация защиты информации". Определение понятия по целям, по функциям, по структуре и т.д. Понятие "режим защиты информации". Режим защиты информации как составная часть организационной защиты информации. Понятие "система организационной защиты информации"; субъекты и объекты системы.

Особенности системы организационной защиты информации, составляющей государственную и коммерческую тайну. Отличительные особенности системы организационной защиты государственной и коммерческой тайны, обусловленные характером защищаемой информации и правом собственности на нее.

Организационные особенности: распределение функций ОЗИ и их структуры. Организационно-правовые особенности: распределение между уровнями государственного управления процессами ОЗИ прав на регулирование процессов защиты, санкций и ответственности, предусмотренных законодательством.

Тема 2. Аналитическая работа как основа управления системой организационной защиты информации

Понятие, цели и задачи аналитической работы по защите информации. Методики аналитической работы, обеспечивающие управляемость системы организационной защиты информации. Технология аналитической работы, ее основные этапы. Формы распространения и использования результатов аналитического исследования.

Использование аналитических методов при определении объектов и субъектов защиты, их взаимоотношений, при проектировании построения, функционировании и оценке эффективности системы организационной защиты информации.

Тема 3. Планирование процессов организационной защиты информации

Планирование процессов организационной защиты информации Сущность планирования как одной из основных функций управления системой организационной защиты информации. Цели планирования. Оценка и анализ состояния системы ОЗИ как основа планирования.

Стратегические и тактические планы. Соотношение планов ОЗИ с планами организа-ции. Разновидности планов; их содержание и форма.

Методы планирования. Особенности программно-целевого планирования.

3.2.3. Требования к уровню освоения содержания модуля

В результате освоения блока слушатель должен:

Знать: принципы и методы организационной защиты информации; базовый понятийный аппарат дисциплины; теоретические основы функционирования систем организационной защиты информации, ее современные проблемы и терминологию; цели, функции и процессы управления системами организационной защиты информации в организациях с различными формами собственности; основные направления и методы организационной защиты информации.

Уметь: анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития; разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации; организовывать работу с персоналом, обладающим конфиденциальной информацией; организовывать охрану персонала, территорий, зданий, помещений и продукции организаций; организовывать и проводить служебное расследование по фактам разглашения, утечки информации и несанкционированного доступа к ней; организовывать и проводить аналитическую работу по предупреждению утечки конфиденциальной информации.

Владеть: методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

3.3. Инженерно-техническая защита информации

3.3.1. Цели и задачи:

формирование профессиональных навыков, связанных с физическими и инженерными принципами обеспечения информационной защиты, с потенциальными возможностями нарушителя по несанкционированному доступу и съему информации по техническим каналам утечки информации, с методами и средствами инженерно-технической защиты информации, с принципом действия, характеристиками и функциональными возможностями технических средств защиты информации, и подготовка к деятельности, связанной с эксплуатацией и обслуживанием современных технических средств защиты информации.

3.3.2. Тематическое содержание дисциплины

№	Наименование дисциплин и тем	Всего часов
1	Основные параметры и характеристики стандартных каналов электрорадиосвязи	2 (Л)
2	Каналы утечки аудиовидеоинформаци	2 (ЛЗ)
3	Устройства скрытого съема аудиовидеоинформации	4 (ЛЗ)
4	Противодействие утечке компьютерной и аудиовидеоинформации	2 (ЛЗ)
Итого		2 (Л), 8 (ЛЗ)

Примечание: Л – лекции, ЛЗ – лабораторные занятия

Тема 1. Основные параметры и характеристики стандартных каналов электрорадиосвязи

Аналоговый канал. Входное и выходное сопротивления и их допустимые отклонения от нормальных значений. Остаточное затухание канала. Частотная характеристика остаточного затухания и эффективно передаваемая полоса частот. Частотная характеристика фазового сдвига между выходным и входным сигналами. Амплитудная характеристика. Уровень помех в точке с нулевым измерительным уровнем. Средний и пиковый уровни мощности сигнала в точке с нулевым измерительным уровнем и динамический диапазон канала. Пропускная способность канала.

Стандартный цифровой канал. Дискретизация. Теорема В.А.Котельникова. Квантование сигнала. Шум квантования. Кодирование. Кодовая комбинация.

Широкополосный канал. Эффективно передаваемая полоса частот. Входное и выходное сопротивления. Средняя мощность сигнала в точке с нулевым измерительным уровнем. Пропускная способность магистрали. Принцип преобразования аналогового сигнала в цифровой с импульсно-кодовой модуляцией.

Тема 2. Каналы утечки аудиовидеоинформации

Классификация каналов утечки информации: акустические, визуально-оптические, электромагнитные, материально-вещественные.

Физические преобразователи аудиовидеоинформации. Параметры преобразователей: чувствительность, разрешающая способность, линейность, инерционность, полоса частот. Индуктивные преобразователи. Емкостные преобразователи. Пьезоэлектрический эффект. Оптические преобразователи.

Излучатели электромагнитных колебаний. Низкочастотные и высокочастотные излучатели.

Паразитные связи и наводки. Паразитные емкостные связи. Паразитные индуктивные связи. Паразитные электромагнитные связи. Паразитные электромеханические связи. Обратная связь в устройствах звуковых частот. Паразитные обратные связи через источники питания. Утечка информации по цепям заземления. Взаимные влияния в линиях связи.

Тема 3. Устройства скрытого съема аудиовидеоинформации

Пассивные и активные способы добычи информации.

Акустическое подслушивание. Разборчивость речи. Реверберация звука. Ослабление звуковых колебаний. Шумы и помехи. Приемные датчики. Прогнозируемая расчетная разборчивость.

Активные способы добычи информации: индуктивный съем информации с телефонной линии, высокочастотное навязывание, установка радиозакладок.

Излучения и наводки от средств видеотехники. Дистанционный аудиовидеоконтроль.

Современный ассортимент прослушивающих устройств.

Тема 4. Противодействие утечке компьютерной и аудиовидеоинформации

Пассивное противодействие. Фильтры и экранирование. Защита телефонных аппаратов. Защита линий связи. Защита от встроенных и узконаправленных микрофонов. Защита от лазерных прослушивающих устройств. Обнаружение радиоизлучений и шумовое противодействие. Нелинейные радиолокаторы.

Примеры приборов противодействия утечке компьютерной и аудиовидеоинформации: устройства зашумления и подавления ПЭМИН, индикаторы поля, многофункциональные системы обнаружения, широкополосные сканирующие приемники, устройства защиты от снятия информации лазерным микрофоном и стетоскопами, устройства постановки помех по силовой сети 220 В.

3.3.3. Требования к уровню освоения содержания модуля

В результате освоения блока слушатель должен:

Знать: технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты.

Уметь: описывать (моделировать) объекты защиты; выявлять и оценивать угрозы безопасности информации на конкретных объектах; определять рациональные меры защиты на объектах и оценивать их эффективность; контролировать эффективность мер инженерно-технической защиты информации.

Владеть: методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.

3.4. Защита информации в компьютерных системах

3.4.1. Цели и задачи:

заложить методически правильные основы знаний по информационной безопасности (ИБ), необходимых специалистам, занимающимся вопросами проектирования, внедрения и эксплуатации корпоративных вычислительных и информационных систем (ВС/ИС).

3.4.2. Тематическое содержание дисциплины

№	Наименование дисциплин и тем	Всего часов
1	Основные положения теории информационной безопасности телекоммуникационных систем	2 (Л), 2 (ЛЗ)
2	Основные технологии построения защищенных телекоммуникационных систем	4 (ЛЗ)
Итого		2 (Л), 6 (ЛЗ)

Примечание: Л – лекции, ЛЗ – лабораторные занятия

Тема 1. Основные положения теории информационной безопасности телекоммуникационных систем

Жизненный цикл конфиденциальной информации (КИ). Информационные угрозы и обеспечение ИБ. Классификация методов защиты КИ. Виды представления КИ и каналы утечки КИ. Источники утечки КИ и демаскирующие признаки в инфокоммуникационной системе (ИКС).

Нормативно-методическое обеспечение создания телекоммуникационных систем. Жизненный цикл телекоммуникационных систем. Модели жизненного цикла телекоммуникационных систем.

Тема 2. Основные технологии построения защищенных телекоммуникационных систем

Этапы проектирования защищенных телекоммуникационных систем. Общая характеристика процесса проектирования. Общие принципы проектирования телекоммуникационных систем. Управление процессом проектирования. Подходы к декомпозиции процесса проектирования. Показатели качества процесса проектирования. Проектная документация.

Методы и методики оценки качества комплексных систем информационной безопасности.

Особенности эксплуатации комплексных систем информационной безопасности на объекте защиты.

3.4.3. Требования к уровню освоения содержания модуля

В результате освоения блока слушатель должен:

Знать: принципы построения информационных систем; предпосылки формирования сферы знаний по информационной безопасности; законодательную и нормативную базу ИБ; основные меры, направленные на обеспечение ИБ на различных уровнях деятельности современного предприятия; иметь полное представление о значение информационной безопасности для современного бизнеса, о перспективах развития технологий обеспечения информационной безопасности.

Уметь: анализировать и выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ; использовать знания о современной методологии управления ИБ для разработки реальных методов формирования защиты информационной инфраструктуры; применять эти методы для формирования и применения политик ИБ предприятия для эффективного управления процессами, работами и процедурами обеспечения ИБ; ориентироваться в инфраструктуре проекта по разработке и внедрению средств, реализующих ИБ.

Владеть: способностью применять на практике международные и российские профессиональные стандарты информационной безопасности, современные парадигмы и методологии, инструментальные средства реализации ИБ; способностью разрабатывать концепцию, программу, политику информационной безопасности предприятия; организовывать и проводить аудит ИБ; использовать современные инструментальные средства анализа рисков и разработки политики ИБ; навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности.

4. Учебно-методическое обеспечение

4.1. Основная литература (учебники и учебные пособия)

1. Ковалёва Н.Н. Информационное право России: учебное пособие – М.: Дашков и К, 2007. – 358 с.
2. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право. – СПб.: Изд-во «Юридический центр Пресс», 2005. – 725с.
3. Копылов В.А. Информационное право: Учебник. – М.: Юристъ, 2004. – 512с.
4. Тедеев А.А. Информационное право (право Интернета) – М.: Эксмо, 2005.
5. Торокин А.А. Техническая защита информации. М.: Гелиос АРВ, 2005. – 960 с.
6. Ярочкин В.И. Информационная безопасность: Учебник. – М.: Трикста, 2005. – 544 с.
7. Акустика: Учебник для вузов / Под ред. Проф. Ю.А.Ковалгина. – М.: Горячая линия – Телеком, 2009. – 660 с.
8. Технические средства и методы защиты информации. Учебное пособие для вузов / А.П.Зайцев, А.А.Шелупанов, Р.ВМещеряков и др. – М.: Горячая линия – Телеком, 2009. – 616 с.
9. Буйневич М.В. Информационная безопасность и защита информации в компьютерных системах: Учебное пособие – Липецк: ЛГПУ, 2007.

4.2. Дополнительная литература

1. Бачило И. Л. Информационное право: Основы практической информатики: Учебное пособие. М., 2001.
2. Близнец И.А. Правовое обеспечение интеллектуальной собственности. Учебно-методическое пособие. М.. 2000.
3. Государственная тайна в Российской Федерации: Учебно-методическое пособие / Под ред. М. А. Вуса. СПб.: Изд-во СПбГУ, 2000.

4. Информационное общество: Информационные войны. Информационное управление. Информационная безопасность / Под ред. М. А. Вуса. СПб.: ФЦП “Интеграция”: Изд-во СПбГУ, 1999.
5. Комментарий к федеральному закону «Об информации, информатизации и защите информации»/ Под ред. И.Л. Бачило, А.В. Волокитина, В.А. Копылова, Б.В. Кристального, Ю.А. Нисневича. – М., 1996.
6. Белов Е.Б. и др. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2006. – 544 с.
7. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки: Учебное пособие. – М.: Изд. Центр РГГУ, 2002. – 399 с.
8. Журавлева Л.В. Радиоэлектроника: Учебник. – М.: Академия, 2005.
9. Комплексная система защиты информации на предприятии учеб. пособие для вузов Н. В. Гришина, В. В. Чудовский - М. Академия, 2009 - 412 с. ил.
10. Методы и средства защиты информации В. А. Хорошко, А. А. Чекатков; под ред Ю. С. Ковтанюка - Киев Юниор, 2003 - 504 с. ил.
11. Обнаружение хакерских атак. Для профессионалов Дж. Чирилло; пер. с англ. А. Ярцева - СПб. Питер, 2003 - 864 с.

4.3. Базы данных, информационно-справочные и поисковые системы

1. http://rpio.ru/ – Российский портал информатизации образования
2. http://www.intuit.ru/ – Национальный Открытый Университет «ИНТУИТ»
3. http://ito.edu.ru/ – Конгресс «Информационные технологии в образовании»
4. http://window.edu.ru/ – Информационная система «Единое окно доступа к образова-тельным ресурсам»
5. http://www.itleader.ru/ – Ежегодный деловой Форум «IT-ЛИДЕР»

4.4. on-line библиотеки

1. http://www.gaudeamus.omskcity.com/ – Омский портал-лаборатория электронной учебной литературы
2. http://www.internet-biblioteka.ru/ – Интернет-библиотека.ру
3. http://litru.ru/ – Электронная библиотека
4. http://sbiblio.com – Библиотека учебной и научной литературы

5. Формы аттестации

При проведении итоговой аттестации используются система «зачет» и «незачет» в соответствии с критериями оценивания, указанными в п.5.2.2.

5.1. Итоговая аттестация

5.1.1. Итоговая аттестация осуществляется после освоения всех дисциплин программы.

5.1.2. Итоговая аттестация проводится аттестационной комиссией, которая оценивает результат выполнения итоговой аттестации как одного из главных показателей эффективности обучения слушателей и принимает решение о выдаче слушателям, успешно освоившим программу и прошедшим итоговую аттестацию, документ об окончании обучения (удостоверение, сертификат).-

5.1.3. Лицам, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть программы и (или) отчисленным из ФГБОУ ВО «ЛГПУ имени П.П. Семенова-Тян-Шанского», выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому ФГБОУ ВО «ЛГПУ имени П.П. Семенова-Тян-Шанского».

5.2. Оценочные материалы

5.2.1. Перечень вопросов для собеседования для итоговой аттестации

1. Основы нормативно-методического обеспечения создания телекоммуникационных систем.
2. Каков жизненный цикл телекоммуникационных систем?
3. Какие модели жизненного цикла телекоммуникационных систем наиболее распространены?
4. Оценка процессов создания телекоммуникационных систем.
5. В чем заключаются основные принципы проектирования телекоммуникационных систем?
6. В чем заключаются общая постановка задачи управления процессом проектирования?
7. Какие подходы к декомпозиции процесса проектирования есть?
8. Перечислите показатели качества процесса проектирования.
9. Назовите основные свойства конфиденциальной информации (КИ) как объекта защиты информации.
10. Охарактеризуйте жизненный цикл КИ.
11. В чем заключается взаимодействие источников КИ с внешней средой?
12. Общие принципы обеспечения инфокоммуникационной безопасности.
13. Перечислите основные информационные угрозы.
14. Виды информации, защищаемой техническими средствами.
15. Свойства информации, влияющие на возможность ее защиты. Полезность и цена информации.
16. Понятие об источниках, носителях и получателях информации. Классификация источников информации.
17. Способы записи информации на различные виды носителей. Виды модуляции сигналов. Характеристики модулированных сигналов.
18. Виды угроз и способы добывания защищаемой информации. Демаскирующие признаки объектов защиты.
19. Аппаратный комплекс LKZ-700. Цели, основные функции. Основные режимы работы генератора и приемника.
20. Анализатор спектра СК-4 Белан. Цели, основные функции. Процедура установки параметров СК-4 Белан для исследования и измерения спектра.
21. Генератор АНР-1001. Цели, основные функции.
22. Сравнительная характеристика физических линий передачи информации. Системы двухпроводной телефонной связи.
23. Роль разведки в деятельности государств и коммерческих структур. Цели и задачи технической разведки.

24. Принципы организации и ведения технической разведки. Общая классификация технической разведки.

25. Элементы акустики речи и акустики помещений. Уровень громкости, логарифмические единицы. Особенности акустики закрытых помещений. Звукоизоляция помещений.

26. Акустоэлектрические приборы (микрофоны). Электроакустические преобразователи (динамики), свойство обратимости.

27. Способы и средства наблюдения. Структура и основные характеристики средств наблюдения. Добывание информации с помощью визуально-оптических и фотографических средств.

28. Оптическая и оптико-электронная разведка. Средства противодействия.

29. Лазеры, основные виды, принципы устройства и работы. Лазерная разведка и разведка лазерных излучений.

30. Радиоэлектронная разведка. Средства противодействия.

31. Виды и способы информационного скрытия речевой информации. Скремблеры. Вокодеры.

32. Гидроакустическая и акустическая разведка. Средства противодействия.

33. Радиационная и химическая разведка. Средства противодействия.

34. Сейсмическая и магнитометрическая разведка. Средства противодействия.

35. Побочные электромагнитные излучения и наводки (ПЭМИН). Способы и средства предотвращения утечки информации через ПЭМИН.

36. Способы и средства технической защиты объектов. Системы охранной и охранно-пожарной сигнализации.

37. Системы и средства контроля и управления доступом (СКУД). Периферийное оборудование и носители информации СКУД. Средства идентификации и аутентификации. Функциональные возможности СКУД.

38. Виды угроз информационной безопасности

39. Источники угроз информационной безопасности

40. Задачи обеспечения информационной безопасности в различных сферах деятельности

41. Методы обеспечения информационной безопасности Российской Федерации в различных сферах

42. Функции и структура государственной системы обеспечения информационной безопасности

43. Концепция построения системы безопасности предприятия. Общая характеристика организационных методов защиты информации.

44. Концепция построения системы безопасности предприятия. Требования к построению систем безопасности предприятия.

45. Концепция построения системы безопасности предприятии. Концептуальная модель информационной безопасности.

46. Концепция построения системы безопасности предприятии. Виды объектов защиты.

47. Концепция построения системы безопасности предприятии. Классификация угроз информационной безопасности и виды каналов утечки информации на предприятии.

48. Концепция построения системы безопасности предприятии. Основные направления организационной защиты информации на предприятии.

49. Действия по защите информации. Характеристика защитных действий.

50. Действия по защите информации. Разглашение защищаемой информации.

51. Действия по защите информации. Способы пресечения разглашения защищаемой информации.

52. Действия по защите информации. Противодействие несанкционированному доступу к информации.

5.2.2. Критерии оценивания

Оценка «зачтено» при итоговой аттестации ставится в случае, если слушатель дает глубокий, осмысленный, полный по содержанию ответ, не требующий дополнений и уточнений. Допускаются такие незначительные недочёты в ответе как отсутствие самостоятельного вывода, нарушение последовательности в изложении, речевые ошибки и др.

Оценка «не зачтено» при итоговой аттестации ставится в случае, если слушатель не может изложить содержание материала, не знает основных понятий. Слушатель испытывает затруднения в установлении связи теории с практикой, не достаточно доказателен в процессе изложения материала, не отвечает на дополнительные и наводящие вопросы преподавателя.

Программа считается освоенной, если успешно пройдена итоговая аттестация.

Составитель программы:

Зияутдинов Владимир Сергеевич, к.п.н., доцент кафедры информатики, информационных технологий и защиты информации.

Программа рассмотрена: на заседании кафедры информатики, информационных технологий и защиты информации (Протокол № __ от «__»_____20__)

Зав. кафедрой информатики, информационных технологий и защиты информации
доцент, кандидат технических наук /Д.М. Скуднев/

Ученого совета ИЕМиТН (Протокол №_ от «__» _____ 201_)

Председатель Ученого совета
доцент, кандидат педагогических наук /В.С.Зиятудинов/

Рецензент:
Власова Лариса Валерьевна, ведущий специалист – эксперт управления труда и занятости Липецкой области (внутреннее рецензирование).

Рецензент:
Скуднев Дмитрий Михайлович, к.т.н., доцент, заведующий кафедрой информатики, информационных технологий и защиты информации (внешнее рецензирование).

Согласовано:

Проректор
по учебной работе — В. С. Зияутдинов

Директор НОЦ — И.Ю. Наумова