МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЛИПЕЦКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ
имени П.П. Семенова-Тян-Шанского»

Дополнительная профессиональная программа
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Аннотация рабочей программы дисциплины 1
Правовая защита информации

Цели и задачи дисциплины:

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

Тематическое содержание дисциплины 1

№	*Наименование тем*	*Всего час.*
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)*	

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.

Аннотация рабочей программы дисциплины 2
Организационная защита информации

Цели и задачи дисциплины:

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.

Тематическое содержание дисциплины 2

№	*Наименование тем*	*Всего час.*
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)*	

Требования к уровню освоения содержания дисциплины:

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.

Аннотация рабочей программы дисциплины 3
Инженерно-техническая защита информации

Цели и задачи дисциплины:
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.

Тематическое содержание дисциплины 3

№	*Наименование тем*	*Всего час.*
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)*	

Требования к уровню освоения содержания дисциплины:
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.

Аннотация рабочей программы дисциплины 4
Защита информаций в компьютерных системах

Цели и задачи дисциплины:
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).

Тематическое содержание дисциплины 4

№	*Наименование тем лекционных занятий*	*Всего час.*
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)*	

Требования к уровню освоения содержания дисциплины:
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.