Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ЛЕСОСИБИРСКИЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ –
филиал Сибирского федерального университета

Утверждаю
Заведующий кафедрой высшей
математики, информатики
и естествознания
_____Л.Н. Храмова
«22» 09 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина «Комплексная система обеспечения информационной безопасности»

Дополнительная образовательная программа профессиональной переподготовки «Информационная безопасность и компьютерная безопасность»

Лесосибирск, 2020

1. Цель освоения дисциплины – формирование у обучающихся знаний и умений комплексного подхода к решению задач информационной безопасности.

Задачи:

– рассмотреть основные общие методологические принципы комплексных систем обеспечения информационной безопасности;

– формировать умение проводить комплексный анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности;

– формировать навыки анализа угроз информационной безопасности.

2. Планируемые результаты обучения

В результате освоения дисциплины обучающийся должен знать:

– основные принципы и методы создания комплексного обеспечения информационной безопасности автоматизированных систем;

– требования и нормативную базу в области защиты информации.

В результате освоения дисциплины обучающийся должен уметь:

– развертывать комплексную систему защиты информации в автоматизированных системах;

– строить политики безопасности автоматизированных систем в соответствии с критериями и требованиями нормативных документов.

В результате освоения дисциплины обучающийся должен владеть:

– навыками работы с нормативными документами в области информационной безопасности;

– подходами к проектированию и внедрению комплекса защитных мер в автоматизированных системах.

3. Содержание дисциплины

№ п/п	Наименование темы и ее содержание	Количество часов
1	Сущность и задачи комплексной защиты информации. Состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ), функциональные и обеспечивающие подсистемы, технология, управление.	20
2	Этапы проектирования КСИБ. Типовые структуры КСИБ. Предпроектное обследование, техническое задание, техническое проектирование, рабочее проектирование, испытания и внедрение в эксплуатацию, сопровождение; особенности проектирования на современном уровне и синтез КСИБ.	25
3	Методы и методики оценки качества КСИБ. Аттестация КСИБ аттестация по требованиям безопасности; особенности эксплуатации КСИБ на объекте защиты, организационно-функциональные задачи службы безопасности.	25
Итого		70

4. Оценочные средства

Форма аттестации – зачет.

Вопросы к зачету:

1. Основные понятия и определения информационной безопасности. Общие цели и задачи защиты информации.
2. Принципы организации комплексной системы защиты информации. Системно-концептуальный подход к защите информации.
3. Основные требования и основные задачи защиты информации в автоматизированных системах.
4. Действующие стандарты в области информационной безопасности. Содержание и основные позиции. Документационное сопровождение комплексной системы защиты информации (КСЗИ).
5. Направления работ по созданию КСЗИ. Аспекты планирования инженерно-технического обеспечения КСЗИ.
6. Этапы работ по созданию КСЗИ. Определение и анализ объектов защиты. Базовые понятия и элементы. Формализация описания архитектуры автоматизированной системы.
7. Определение и анализ объектов защиты. Определение исходного уровня защищенности.
8. Классификация защищенности АС в соответствии с РД. Основные требования.
9. Оценка угроз ИБ. Выявление способов НСД и каналов утечки информации.
10. Объективные и субъективные факторы, воздействующие на информацию (по ГОСТ).
11. Виды угроз и основные последствия их реализации.
12. Понятие «нарушителя» и модели нарушителя. Классификации.
13. Модель угроз и принцип ее формирования. Базовая модель угроз безопасности персональных данных (ФСТЭК).
14. Модель угроз и принцип ее формирования. Методология формирования модели угроз в соответствии с рекомендациями ФСБ.
15. Методики оценки рисков. Применяемые на практике подходы.
16. Структура процесса управления рисками.
17. Средства защиты информации и механизмы обеспечения безопасности информации. Идентификация и аутентификация.
18. Средства защиты информации и механизмы обеспечения безопасности информации. Разграничение доступа. Регистрация и аудит.
19. Средства защиты информации и механизмы обеспечения безопасности информации. Криптографическая подсистема.
20. Средства защиты информации и механизмы обеспечения безопасности информации. Межсетевое экранирование.
21. Планирование мероприятий КСЗИ.
22. Контроль мероприятий КСЗИ. Основные аспекты.

23. Оценка эффективности КСЗИ. Общая характеристика применяемых методов.

24. Оценка эффективности КСЗИ. Оценочные подходы.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Шаньгин, В.П. Информационная безопасность / В.П. Шаньгин. – Москва, 2015

2. Грибунин, В.Г. Комплексная система защиты информации на предприятии: учеб. пособие для вузов / В.Г. Грибунин, В.В. Чудовский. – Москва : Академия, 2017

Дополнительная литература:

1.Мельников, В.П. Информационная безопасность и защита информации: учеб. пособие для вузов / В.П. Мельников, С.А. Клейменов, А.М. Петраков, С.А. Клейменов. – Москва : Академия, 2015

Разработчик:
Заведующий кафедрой ВМИиЕ,
профессор, кандидат экономических наук,
доцент Л.Н. Храмова

Кандидат педагогических наук,
старший преподаватель кафедры ВМИиЕ А.В. Фирер

Согласовано:

Согласовано:
Декан ФДО Л.С. Шмульская