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 «Компьютерная безопасность»

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

Лесосибирск, 20__

1. Цель освоения дисциплины – изучение основных теоретических положений и методов, формирование умений и привитие навыков применения теоретических знаний для решения прикладных задач, а также развитие новых подходов к обеспечению компьютерной безопасности.

Задачи:

– формирование представления о современных тенденциях угроз компьютерной безопасности;

– формирование умений выявлять угрозы компьютерной безопасности;

– формирование навыков владения приемами разработки политики безопасности предприятия и навыками использования методов и средств обеспечения компьютерной безопасности.

2. Планируемые результаты обучения

В результате освоения дисциплины обучающийся должен знать:

– теоретические основы анализа и обеспечения компьютерной безопасности данных;

– теоретические положения и нормативы по организации и сопровождении работы и аттестации объекта информатизации по требованиям безопасности;

В результате освоения дисциплины обучающийся должен уметь:

– применять комплексный подход к обеспечению компьютерной безопасности;

– осуществлять контроль и аттестацию объекта информатизации по требованиям безопасности информации;

В результате освоения дисциплины обучающийся должен владеть:

– способностью участвовать в работах по реализации политики компьютерной безопасности;

– способами и методами безопасности по организации и сопровождении работы и аттестации объекта информации.

3. Содержание дисциплины

3.1 Содержание дисциплины по программе, общая трудоемкость которой составляет 510 часов.

№ п/п	Наименование темы и ее содержание	Количество часов
1	Международные стандарты информационного обмена. Понятие угрозы. Компьютерная безопасность в условиях функционирования в России глобальных сетей. Три вида возможных нарушений информационной системы. Защита. Современная нормативно-законодательная база обеспечения информационной безопасности. Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация.	20
2	Таксономия нарушений информационной безопасности	25

№ п/п	Наименование темы и ее содержание	Количество часов
	вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности.	
3	Использование защищенных компьютерных систем. Методы криптографии. Основные технологии построения защищенных систем. Место компьютерной безопасности экономических систем в национальной безопасности страны.	25
Итого		70

3.2 Содержание дисциплины по программе, общая трудоемкость которой составляет 260 часов.

№ п/п	Наименование темы и ее содержание	Количество часов
1	Международные стандарты информационного обмена. Понятие угрозы. Компьютерная безопасность в условиях функционирования в России глобальных сетей. Три вида возможных нарушений информационной системы. Защита. Современная нормативно-законодательная база обеспечения информационной безопасности	10
2	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности.	20
3	Использование защищенных компьютерных систем. Методы криптографии. Основные технологии построения защищенных систем. Место компьютерной безопасности экономических систем в национальной безопасности страны.	20
Итого		50

4. Оценочные средства

Форма аттестации – зачет.

Вопросы к зачету:

1.Понятие «компьютерная безопасность». Предпосылки и цели обеспечения информационной безопасности.

2.Национальные интересы РФ в информационной сфере.

3.Информационная борьба и пути решения проблем информационной безопасности РФ.

4.Принципы обеспечения защиты информации.

5.Виды угроз информационной безопасности предприятия (организации).

6.Источники наиболее распространенных угроз информационной безопасности.

7. Виды сетевых атак.

8. Способы снижения угрозы сниффинга пакетов.

9. Меры по устранению угрозы IP –спуфинга.

10. Борьба с атаками на уровне приложений.

11. Проблемы обеспечения безопасности локальных вычислительных сетей.

12. Распределенное хранение файлов.

13.Требования по обеспечению комплексной системы информационной безопасности.

14. Уровни информационной защиты существуют,

15. Задачи криптографии.

16. Многоалфавитная подстановка как схема шифрования.

17. Защита информации от несанкционированного доступа.

18. Достоинства и недостатки программно-аппаратных средств защиты информации.

19. Виды механизмов защиты для обеспечения идентификации и аутентификации пользователей.

20. Задачи подсистемы управления доступом.

21. Требования к подсистеме протоколирования аудита.

22. Виды механизмов защиты для обеспечения конфиденциальности данных и сообщений.

23. Контроль участников взаимодействия.

24. Функции службы регистрации и наблюдения.

25. Информационно-опасные сигналы, их основные параметры.

26. Требования, необходимые при экранировании помещений, предназначенных для размещения вычислительной техники.

27. Понятие «аутентификация пользователя». Схемы аутентификации.

28. Понятие «смарт-карты».

29. Требования к современным криптографическим системам защиты информации.

30. Симметричная криптосистема.

31. Виды симметричных криптосистем.

32. Асимметричная криптосистема.

33. Классификация криптографических алгоритмов по стойкости.

34. Анализ надежности криптосистем.

35. Дифференциальный криптоанализ.

36. Требования к автоматизированным системам защиты третьей группы.

37. Требования к автоматизированным системам защиты второй группы.

38. Требования к автоматизированным системам защиты первой группы.

39. Классы защиты информации от несанкционированного доступа для средств вычислительной техники.

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

Основная литература:

1.Садердинов, А.А. Информационная безопасность предприятия / А.А. Садердинов. – Москва, 2016.

2. Шаньгин, В.А. Информационная безопасность компьютерных систем / В.А. Шаньгин. – Москва, 2015.

Дополнительная литература:

3. Галатенко, В.А. Основы информационной безопасности : учеб. пособие для студентов / В.А. Галатенко. – Москва, 2016

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