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
«_23_» _09_____2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина «Аудит информационной безопасности»

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

Лесосибирск, 2020

1. Цель освоения дисциплины – формирование знаний и навыков, необходимых для организации процедуры аудита информационной безопасности защищённых автоматизированных систем.

Задачи:

– изучение представления о методах сбора и анализа свидетельств аудита информационной безопасности и их оценке;

– формирование навыков использования методологии, стандартов и нормативных требования в области аудита информационной безопасности.

2. Планируемые результаты обучения

В результате освоения дисциплины обучающийся должен знать:

– основы системного подхода к обеспечению информационной безопасности;

– методы системного анализа и математического моделирования, применяемые при оценке информационной безопасности.

В результате освоения дисциплины обучающийся должен уметь:

- осуществлять классификацию задач и процессов информационной безопасности;

– применять методы системного анализа и математического моделирования для аудита информационной безопасности.

В результате освоения дисциплины обучающийся должен владеть:

– стандартными методиками анализа состояния информационной безопасности;

– программными средствами для проведения системного анализа и математического моделирования для аудита информационной безопасности.

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	Основные типы аудита информационной безопасности. Основные возможности современных методик анализа рисков и аудита ИБ. Цели проведения АИБ. Базовые угрозы ИБ, учитываемые при проведении аудита. Особенности проведения внешнего и внутреннего аудита. Основные типы аудита ИБ с учетом охвата им объектов защиты. Особенности сетевого аудита.	4
2	Базовые этапы аудита информационной безопасности. Организационные вопросы, решение которых целесообразно на этапе инициирования процедуры аудита. Базовая документация, необходимая аудиторской группе для выполнения аудита. Основные подходы, используемые аудиторами при анализе данных аудита. Особенности рекомендаций аудиторской группы по итогам аудита. Структура и содержание основных разделов аудиторского отчёта.	6
3	Основные направления аудита информационной безопасности. Основные составляющие аттестации объектов информатизации. Базовые	6

№ п/п	Наименование темы и ее содержание	Количество часов
	компоненты контроля защищенности информации ограниченного доступа. Состав специальных исследований технических средств на наличие побочных электромагнитных излучений и наводок. Особенности проектирования объектов информатизации в защищенном исполнении. Основные виды АИБ. Базовые процедуры, реализуемые при проведении активного аудита.	
4	Правовые аспекты аудита информационной безопасности и программные средства для его реализации. Основные задачи, выполняемые сетевыми сканерами. Особенности сканера XSpider. Базовые аудиторские задачи, реализуемые с помощью CRAMM. Основные компоненты программного обеспечения «АванГард». Международные стандарты и руководства в сфере АИБ. Структура стандарта BS7799. Особенности стандартов ISO17799 и ISO 15408. Структура стандарта COBIT. Основные этапы проведения аудита в соответствии со стандартом COBIT. Особенности стандартов BSI/IT, SYSTRUST и GIAC. Характеристика международных стандартов серии ISO/IEC 27000.	6
5	Общая модель процесса аудита информационной безопасности объекта. Аудит информационной безопасности (организации, автоматизированной системы),аудита информационной безопасности. Назначение, цель аудита информационной безопасности объекта.	6
6	Этапы, процедуры аудита информационной безопасности защищённых автоматизированных систем и организаций. Взаимодействие аудиторской организации с проверяемой организацией. Ответственность аудиторской организации и проверяемой организации. Определение области аудита ИБ, критериев аудита ИБ	8
7	Методы оценки информационной безопасности автоматизированных систем и организаций. Модель оценки ИБ. Методы измерения атрибутов оценки. Способы формирования показателей оценки. Критерии принятия решения формирования результатов оценки. Интерпретация результатов оценки.	6
8	Управление аудитом информационной безопасности. Планирование программы аудита ИБ. Реализация и поддержка программы аудита ИБ. Контроль и совершенствование программы аудита ИБ.	6
9	Международные, национальные и корпоративные стандарты и руководства в области аудита и оценки информационной безопасности. Международные стандарты в области аудита и оценки ИБ. Национальные стандарты и руководства в области аудита и оценки. Российские стандарты в области аудита и оценки ИБ.	6
10	Планирование аудиторской проверки. Планирование аудита, его назначение и принципы. Разработка предварительного и общего плана аудита, аудиторской программы и конкретных аудиторских процедур. Существенность в аудите. Аудиторский риск. Виды риска. Изучение и оценка систем бухгалтерского учета и внутреннего контроля в ходе аудита.	6
Итого		60

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

№ п/п	Наименование темы и ее содержание	Количество часов
1	Основные типы аудита информационной безопасности. Основные возможности современных методик анализа рисков и аудита ИБ. Цели проведения АИБ. Базовые угрозы ИБ, учитываемые при проведении аудита. Особенности проведения внешнего и внутреннего аудита. Основные типы аудита ИБ с учетом охвата им объектов защиты. Особенности сетевого аудита.	2
2	Базовые этапы аудита информационной безопасности. Организационные вопросы, решение которых целесообразно на этапе инициирования процедуры аудита. Базовая документация, необходимая аудиторской группе для выполнения аудита. Основные подходы, используемые аудиторами при анализе данных аудита. Особенности рекомендаций аудиторской группы по итогам аудита. Структура и содержание основных разделов аудиторского отчёта.	4
3	Основные направления аудита информационной безопасности. Основные составляющие аттестации объектов информатизации. Базовые компоненты контроля защищенности информации ограниченного доступа. Состав специальных исследований технических средств на наличие побочных электромагнитных излучений и наводок. Особенности проектирования объектов информатизации в защищенном исполнении. Основные виды АИБ. Базовые процедуры, реализуемые при проведении активного аудита.	6
4	Правовые аспекты аудита информационной безопасности и программные средства для его реализации. Основные задачи, выполняемые сетевыми сканерами. Особенности сканера XSpider. Базовые аудиторские задачи, реализуемые с помощью CRAMM. Основные компоненты программного обеспечения «АванГард». Международные стандарты и руководства в сфере АИБ. Структура стандарта BS7799. Особенности стандартов ISO17799 и ISO 15408. Структура стандарта COBIT. Основные этапы проведения аудита в соответствии со стандартом COBIT. Особенности стандартов BSI/IT, SYSTRUST и GIAC. Характеристика международных стандартов серии ISO/IEC 27000.	4
5	Общая модель процесса аудита информационной безопасности объекта. Аудит информационной безопасности (организации, автоматизированной системы),аудита информационной безопасности. Назначение, цель аудита информационной безопасности объекта.	4
6	Этапы, процедуры аудита информационной безопасности защищённых автоматизированных систем и организаций. Взаимодействие аудиторской организации с проверяемой организацией. Ответственность аудиторской организации и проверяемой организации. Определение области аудита ИБ, критериев аудита ИБ	4
7	Методы оценки информационной безопасности автоматизированных систем и организаций. Модель оценки ИБ. Методы измерения атрибутов оценки. Способы формирования показателей оценки. Критерии принятия решения формирования результатов оценки. Интерпретация результатов	4

№ п/п	Наименование темы и ее содержание	Количество часов
	оценки.	
8	Управление аудитом информационной безопасности. Планирование программы аудита ИБ. Реализация и поддержка программы аудита ИБ. Контроль и совершенствование программы аудита ИБ.	4
9	Международные, национальные и корпоративные стандарты и руководства в области аудита и оценки информационной безопасности. Международные стандарты в области аудита и оценки ИБ. Национальные стандарты и руководства в области аудита и оценки. Российские стандарты в области аудита и оценки ИБ.	4
10	Планирование аудиторской проверки. Планирование аудита, его назначение и принципы. Разработка предварительного и общего плана аудита, аудиторской программы и конкретных аудиторских процедур. Существенность в аудите. Аудиторский риск. Виды риска. Изучение и оценка систем бухгалтерского учета и внутреннего контроля в ходе аудита.	4
Итого		40

4. Оценочные средства

Форма аттестации – экзамен.

Вопросы к экзамен:

1.Аудит информационной безопасности (ИБ): понятие, задачи, цели

2.Стандарты и практики, применяемые в аудит. Базовые принципы аудита ИБ.

3.Критерии ценности аудит-заключения. Основные этапы ИБ-аудита и их содержание. Документы, создаваемые в результате ИБ-аудита.

4.Направления ИБ-аудита. Возможные результаты проведения ИБ-аудита.

5.Информационные технологии, востребованные в современном ИБ-аудите. Помехи ИБ-проектам.

6.Стандарты и методики в области разработки ИБ-аудита.

7.Стандарт ГОСТР 50922-2006: назначение, структура, области применения.

8.Стандарты ISO/IEC 17799:2005: назначение, область применения, структура.

9.Иерархическая структура ИБ-аудита.

10.Анализ требований и определение спецификации ИБ-аудита программного обеспечения. Требования к спецификации.

11.Динамическое программирование в задаче обеспечения ИБ.

12.Понятие надежности. Структура ГОСТ 27 – Надежность в технике.

13.Модели надежности в технике.

14.Свойства, характеризующие надежность.

15.Надежности программного обеспечения. Объекты уязвимости программного обеспечения и дестабилизирующие факторы.

16.Обеспечение надежности на различных этапах жизненного цикла вычислительных систем.

17.Сертификация программного обеспечения. Рынок программных средств.

18.Источники угроз для Интернет-ресурсов и пути их нейтрализации.

19.Мероприятия, обеспечивающие приемлемый уровень ИБ.

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

Основная литература:

1. Дадян, Э.Г. Данные: хранение и обработка: Учебник / Э.Г. Дадян. – Москва, 2019.

2. Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом : учебное пособие / Н.Б.Ельчанинова. – Ростов-на-Дону - Таганрог : Издательство Южного федерального университета, 2017.

Дополнительная литература:

3. Новиков, В.К. Организационно-правовые основы информационной безопасности. Юридическая ответственность за правонарушения в области информационной безопасности : учебное пособие / В.К. Новиков. – Москва, 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