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
«_____»_____2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина «Криптографическая защита информации»

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

Лесосибирск, 2020

1. Цель освоения дисциплины – ознакомление обучающихся с основополагающими принципами криптографических методов и алгоритмов защиты информации, с особенностями применения соответствующих криптосистем.

Задачи:

– изучение принципов синтеза и анализа криптосистем

– формирование системного подхода к организации защиты информации;

2. Планируемые результаты обучения

В результате освоения дисциплины обучающийся должен знать:

– нормативные требования по административно-правовому регулированию в области криптографической защиты информации;

– методы криптографического синтеза и анализа;

– методы криптозащиты компьютерных систем и сетей.

В результате освоения дисциплины обучающийся должен уметь:

– использовать типовые шифры замены и перестановки;

– применять частотные характеристики языков в криптоанализе;

– формулировать требования к шифрам и основные характеристики шифров.

В результате освоения дисциплины обучающийся должен владеть:

– навыком использования основных типов шифров и криптографических алгоритмов;

– методами криптоанализа простейших шифров;

– навыком применения криптографии в решении задач аутентификации, построения систем цифровой подписи.

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 понятия и определения криптологии. Шифры Цезаря, Полибия, Спартанцев. Основные характеристики шифра Цезаря, шифра Полибия и шифра древней Спарты. Основные характеристики шифра простой перестановки и шифра двойной перестановки. Основные характеристики шифра магических квадратов и шифра Гронсфельда. Основные характеристики биграммных шифров. Основные характеристики таблиц Виженера и таблиц Трисемуса	10
2	Шифры простой и двойной перестановок, магического квадрата, Гронсфельда. Шифры простой и двойной перестановок, магического квадрата, Гронсфельда. Таблицы Виженера и Трисемуса. Биграммный шифр Playfair. Биграммный шифр Чарльза Уитстона. Шифровальные машины. Одноразовый шифровальный блокнот. Основные характеристики биграммного шифра Playfaiи биграммного	10

№ п/п	Наименование темы и ее содержание	Количество часов
	шифра Чарльза Уитстона. Шифровальные машины. Одноразовый шифровальный блокнот.	
3	Симметричные криптосистемы. Перестановки. Моноалфавитные и многоалфавитные подстановки. Системы шифрования Виженера. Псевдослучайные генераторы. Гаммирование. Стандарты шифрования DES и ГОСТ. Моноалфавитные многоалфавитные подстановки. Системы шифрования Виженера. Псевдослучайные генераторы. Алгоритмы гаммирования. Стандарты шифрования DES и ГОСТ.	10
4	Модели асимметричных криптосистем. Двух-ключевые системы шифрации. Однонаправленные функции. Алгоритм RSA. Криптографические хэш функции. Криптосистемы на эллиптических ключах. Изучение ассиметричных криптосистем, процедур аутентификации и ЭЦП. Криптосистемы без передачи ключей.	10
5	Электронная цифровая подпись. Криптографические хэш-функции. Электронная цифровая подпись и ее алгоритмы. Распределение ключей. Методы экспоненциального ключевого обмена. Цифровая подпись, протоколы аутентификации.	10
6	Протоколы аутентификации. Методы разграничения доступа. Аутентификация и идентификация. Модели и методы разграничения доступа. Модели и методы удаленной аутентификации.	10
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 понятия и определения криптологии. Шифры Цезаря, Полибия, Спартанцев. Основные характеристики шифра Цезаря, шифра Полибия и шифра древней Спарты. Основные характеристики шифра простой перестановки и шифра двойной перестановки. Основные характеристики шифра магических квадратов и шифра Гронсфельда. Основные характеристики биграммных шифров. Основные характеристики таблиц Виженера и таблиц Трисемуса	6
2	Шифры простой и двойной перестановок, магического квадрата, Гронсфельда. Шифры простой и двойной перестановок, магического квадрата, Гронсфельда. Таблицы Виженера и Трисемуса. Биграммный шифр Playfair. Биграммный шифр Чарльза Уитстона. Шифровальные машины. Одноразовый шифровальный блокнот. Основные характеристики биграммного шифра Playfaiи биграммного шифра Чарльза Уитстона. Шифровальные машины. Одноразовый шифровальный блокнот.	6
3	Симметричные криптосистемы. Перестановки. Моноалфавитные и многоалфавитные подстановки. Системы шифрования Виженера. Псевдослучайные генераторы. Гаммирование. Стандарты шифрования DES и ГОСТ. Моноалфавитные и многоалфавитные подстановки. Системы шифрования Виженера. Псевдослучайные генераторы. Алгоритмы гаммирования. Стандарты шифрования DES и ГОСТ.	6

№ п/п	Наименование темы и ее содержание	Количество часов
4	Модели асимметричных криптосистем. Двух-ключевые системы шифрации. Однонаправленные функции. Алгоритм RSA. Криптографические хэш функции. Криптосистемы на эллиптических ключах. Изучение ассиметричных криптосистем, процедур аутентификации и ЭЦП. Криптосистемы без передачи ключей.	8
5	Электронная цифровая подпись. Криптографические хэш-функции. Электронная цифровая подпись и ее алгоритмы. Распределение ключей. Методы экспоненциального ключевого обмена. Цифровая подпись, протоколы аутентификации.	8
6	Протоколы аутентификации. Методы разграничения доступа. Аутентификация и идентификация. Модели и методы разграничения доступа. Модели и методы удаленной аутентификации.	6
Итого		40

4. Оценочные средства

Форма аттестации – экзамен.

Вопросы к экзамену:

1.Основные характеристики шифра Цезаря, шифра Полибия и шифра древней Спарты.

2.Основные характеристики шифра простой перестановки и шифра двойной перестановки.

3.Основные характеристики биграммных шифров.

4.Основные характеристики таблиц Виженера и таблиц Трисемуса

5.Шифры простой и двойной перестановок, магического квадрата, Гронсфельда.

6.Биграммный шифр Playfair.

7.Биграммный шифр Чарльза Уитстона.

8.Шифровальные машины.

9.Одноразовый шифровальный блокнот.

10. Перестановки. Моноалфавитные и многоалфавитные подстановки.

11. Системы шифрования Виженера.

12.Псевдослучайные генераторы.

13. Гаммирование.

14.Стандарты шифрования DES и ГОСТ.

15.Моноалфавитные и многоалфавитные подстановки.

16.Модели асимметричных криптосистем.

17.Двух-ключевые системы шифрации.

18.Однонаправленные функции. Алгоритм RSA.

19.Криптографические хэш функции.

20.Криптосистемы на эллиптических ключах.

21.Изучение ассиметричных криптосистем, процедур аутентификации и ЭЦП.

22.Криптосистемы без передачи ключей.

23.Электронная цифровая подпись.

24. Электронная цифровая подпись и ее алгоритмы.

25.Распределение ключей. Методы экспоненциального ключевого обмена.

26.Цифровая подпись, протоколы аутентификации Протоколы аутентификации.

27.Методы разграничения доступа. Аутентификация и идентификация.

28.Модели и методы разграничения доступа. Модели и методы удаленной аутентификации.

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

Основная литература:

1.Ожиганов, А.А. Криптография : учебное пособие. / Ожиганов А.А. – Санкт-Петербург, 2016.

2.Ожиганов, А.А. Криптографические системы с секретным и открытым ключом : учебное пособие / А.А. Ожиганов. – Санкт-Петербург, 2015.

Дополнительная литература:

3.Бабаш, А.В. Криптографические методы защиты информации : учебник / А.В. Бабаш, Е.К. Баранова. – 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