УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

АЛТАЙСКИЙ ФИЛИАЛ

УТВЕРЖДАЮ
Директор филиала

_____В.А. Иванова

«26» апреля 2022 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
Основы криптографии

(наименование дисциплины)

Направление подготовки	**09.03.03 «Прикладная информатика»**
Профиль(и)/направленность	**Прикладные информационные системы в экономике и финансах**
Ответственный за актуализацию РПД	**Останин С.А.**
Год утверждения РПД	**2022 г.**

(основной РПД)

СОДЕРЖАНИЕ

1. Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине 3
2. Перечень вопросов, заданий, тем для подготовки к текущему контролю 6

1 Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с компетенциями/индикаторам и достижения компетенции
ПКН-2	Способность разрабатывать алгоритмы и программы с использованием современных технологий программирования	1. Владеет объектно-ориентированным языком программирования на уровне знания синтаксиса и семантики, основ стандартной библиотеки.	**Знать** основы современных объектно- ориентированных языков программирования. **Уметь** использовать современные технологий программирования и стандартные библиотеки.
		2. Использует инструментальные средства программирования (IDE, SDK, API, популярные фреймворки и библиотеки).	**Знать** современные инструментальные средства программирования. **Уметь** использовать популярные фреймворки и стандартные библиотеки для достижения высокой скорости разработки проектов по обеспечению безопасности данных.
		3. Организовывает кодовую базу, ориентируется в существующем коде, демонстрирует знание общепринятых соглашений и политик в области оформления кода. 4. Проектирует текстовый, программный или графический интерфейс программной системы исходя из ее назначения.	**Знать** принципы организации кодовой базы. **Уметь** ориентироваться в существующем коде, и демонстрировать знание общепринятых соглашений и политик безопасности в области оформления кода. **Знать** принципы проектирования программного и графического интерфейса программной системы с учетом требований информационной безопасности. **Уметь** настраивать программный или графический интерфейс системы исходя из ее назначения.

ПКН-7	Способность выполнять сервисное обслуживание и настройку аппаратного и программного обеспечения, в том числе с учетом требований информационной безопасности	1. Демонстрирует знание основ функционирования компьютерной техники, решет часто возникающие проблемы в их эксплуатации, выполняет первичную установку и настройку популярных программ и операционных систем. 2. Демонстрирует знание основ функционирования операционных систем и компьютерных сетей, настраивает сетевые подключения и службы, диагностирует их работу и решет типичные задачи администрирования сетей. 3. Использует серверные операционные системы для разработки и развертывания сетевых приложений, настраивает веб-службы, частично автоматизирует эти процессы.	**Знать** основы функционирования компьютерной техники и возникающие проблемы в их эксплуатации. **Уметь** выполнять первичную установку и настройку популярных программ и операционных систем с учетом требований информационной безопасности. **Знать** основы функционирования операционных систем и компьютерных сетей с учетом требований информационной безопасности. **Уметь** решать типовые задачи администрирования сетей с учетом требований по шифрованию данных. **Знать** основы функционирования серверных операционных систем для разработки и развертывания сетевых приложений, с учетом требований информационной безопасности. **Уметь** развертывать сетевые приложения, и обеспечивать настройку веб-приложений с учетом требований по шифрованию данных.

		4. Демонстрирует знание основ компьютерной безопасности, алгоритмов шифрования, хеширования, понятий аутентификации, авторизации, цифровых сертификатов, протоколов безопасной передачи данных.	**Знать** основы компьютерной безопасности информационно-телекоммуникационных сетей. **Уметь** использовать современные алгоритмы шифрования, хеширования, идентификации и аутентификации.

2. Перечень вопросов, заданий, тем для подготовки к текущему контролю

1. Криптография (определение).
2. Криптоанализ (определение).
3. Криптографическая система (определение).
4. Примеры шифрующих устройств до нашей эры.
5. К какому классу относится шифр Цезаря?
6. Одноалфавитный метод шифрования и пример шифрования.
7. Шифрование методом перестановки символов.
8. Многоалфавитные методы шифрования и пример шифрования.
9. Метод гаммирования.
10. Какой размер ключа в отечественном стандарте симметричного шифрования?
11. Теоретически стойкие шифры (определение).
12. Кольцо целых чисел (определение).
13. Кольцо целых чисел по модулю n (определение).
14. Как вычислить (зашифровать) значение зашифрованного сообщения (число) c, если известно исходное сообщение (число) m, и открытый ключ RSA (e, n)?
15. Как расшифровать (вычислить) значение расшифрованного сообщения (число) m, если известно зашифрованное сообщение (число) c, и закрытый ключ RSA (d, n)?

Ответы на вопросы

1. Криптография (определение).

Ответ

Криптография - наука о создании безопасных методов связи, о создании стойких (устойчивых к взлому) шифров. Она занимается поиском математических методов преобразования информации.

2. Криптоанализ (определение).

Ответ

Криптоанализ **-** раздел, посвященный исследованию возможности чтения сообщений без знания ключей, то есть связан непосредственно со взломом шифров.

3. Криптографическая система (определение).

Ответ

Криптографическая система - семейство преобразований шифра и совокупность ключей. Само по себе описание алгоритма не является криптосистемой. Только дополненное схемами распределения и управления ключами оно становится системой. Криптосистема работает по определенной методологии (процедуре). Она состоит из одного или более алгоритмов шифрования, ключей, используемых этими алгоритмами шифрования, системы управления ключами, незашифрованного текста и зашифрованного текста.

4. Примеры шифрующих устройств до нашей эры

Ответ

Сцилата, квадрат Полибия.

5. К какому классу относится шифр Цезаря?

Ответ

Шифр Цезаря относится к так называемому классу моноалфавитных подстановок.

6. Одноалфавитный метод шифрования и пример шифрования.

Ответ

В основе одноалфавитного метода шифрования лежит простой способ шифрования: отправитель и получатель зашифрованного документа заранее договариваются об определенном смещении букв относительно их обычного местоположения в алфавите. Например, для кириллицы, если смещение равно 1, то А соответствует букве Б, Б - В и т. д., а когда алфавит подходит к концу, то начинают брать буквы из начала списка. И выходит, например, следующее: из слова КОДИРОВАНИЕ получается ЛПЕЙСПГБОЙЖ.

7. Шифрование методом перестановки символов

Ответ

Метод заключается в том, что символы текста переставляются по определенным правилам, при этом используются только символы исходного (незашифрованного) текста

8. Многоалфавитные методы шифрования и пример шифрования.

Ответ

Многоалфавитное шифрование (многоалфавитная замена) заключается в том, что для последовательных символов шифруемого текста используются одноалфавитные методы с различными ключами. Например, первый символ заменяется по методу Цезаря со смещением 14, второй — со смещением 10 и т. д. до конца заданного ключа. Затем процедура продолжается периодически.

9. Метод гаммирования

Ответ

Данный способ преобразования заключается в том, что символы закрываемого текста последовательно складываются с символами некоторой специальной последовательности именуемой гаммой. Такое преобразование иногда называют наложением гаммы на открытый текст.

10. Какой размер ключа в отечественном стандарте симметричного шифрования?

Ответ

256 бит.

11. Теоретически стойкие шифры (определение)

Ответ

Шифры, для которых средняя вероятность правильного декодирования открытого сообщения с заданной многозначностью по шифрованному тексту стремится к нулю с ростом длины сообщения.

12. Кольцо целых чисел (определение).

Ответ

Множество всех целых чисел с операциями сложения и умножения.

13. Кольцо целых чисел по модулю *n* (определение).

Ответ

Множество чисел $Z/n=\{0, 1, 2, \ldots, (n-1)\}$ с операциями сложения и умножения по модулю n.

14. Как вычислить (зашифровать) значение зашифрованного сообщения (число) *c*, если известно исходное сообщение (число) *m*, и открытый ключ RSA (*e*, *n*)?

Ответ

Зашифровать сообщение с использованием открытого ключа следует следующим образом:

$$c = E(m) = m^e \bmod n$$

15. Как расшифровать (вычислить) значение расшифрованного сообщения (число) *m*, если известно зашифрованное сообщение (число) *c*, и закрытый ключ RSA (*d*, *n*)? Ответ

Расшифровать сообщение с использованием открытого ключа следует следующим образом:

$$m = D(c) = c^d \bmod n$$

Критерии балльной оценки различных форм текущего контроля успеваемости

Вид учебной деятельности	*Баллы*	*Примечание*
Выступление по вопросу на семинарском занятии	До 5	20 баллов до 15 ноября
Аудиторная практическая работа	До 11	
Посещаемость	До 4	
Аудиторная практическая работа	До 11	20 баллов до 30 декабря
Письменная работа	До 5	
Посещаемость	До 4	
Итого	**40**	За семестр

Порядок перевода 100-балльной оценки в пятибалльную

100-балльная система	**5-балльная система**
50-100	зачтено
менее 50	не зачтено
86-100	отлично
70-85	хорошо
50-69	удовлетворительно

Менее 50	неудовлетворительно

Студент считается аттестованным при условии, что сумма баллов за работу в семестре (модуле) и ответ на зачете/экзамене составляет не менее 51 балла.