МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Майкопский государственный технологический университет»

Факультет информационных систем в экономике и юриспруденции

Кафедра информационной безопасности и прикладной информатики

УТВЕРЖДАЮ
Проректор по учебной работе
_____Л. И. Задорожная
«25»____10_____ 2017 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.Б.19 Криптографические методы защиты информации

по специальности 10.05.04 Информационно-аналитические системы безопасности

специализация №2 Информационная безопасность финансовых и экономических струтур

Квалификация (степень) выпускника Специалист

Уровень подготовки Специалитет

Форма обучения Очная

Год начала подготовки 2018

Майкоп

Рабочая программа составлена на основе ФГОС ВО и учебного плана МГТУ по направлению (специальности) 10.05.04 Информационно-аналитические системы безопасности

Составитель рабочей программы:

Доцент кафедры, к.ф.-м.н. _____ Киздермишов А.А.
(должность, ученое звание, степень) (подпись) (Ф.И.О.)

Рабочая программа утверждена на заседании кафедры

Информационной безопасности и прикладной информатики
(наименование кафедры)

Заведующий кафедрой
«25»____10_____ 2017 г.. _____ Чефранов С.Г.
(подпись) (Ф.И.О.)

Одобрено учебно-методической комиссией факультета
(где осуществляется обучение) «25»____10_____ 2017 г.

Председатель
учебно-методического
совета направления
(где осуществляется обучение) _____ Чефранов С.Г.
(подпись) (Ф.И.О.)

Декан факультета
(где осуществляется обучение)
«25»____10_____ 2017 г. _____ Доргушаова А.К..
(подпись) (Ф.И.О.)

СОГЛАСОВАНО:
Начальник УМУ
«25»____10_____ 2017 г. _____ Чудесова Н.Н.
(подпись) (Ф.И.О.)

Зав. выпускающей кафедрой
по направлению _____ Чефранов С.Г.
(подпись) (Ф.И.О.)

1. Цели и задачи освоения дисциплины

Цель изучения дисциплины - «Криптографические методы защиты информации» формирование знаний об основных подходах, методах и алгоритмах современной криптологии.

Основные задачи дисциплины:

- обучение студентов математическим основам криптографии, базовым принципам работы симметричных и асимметричных криптографических систем при использовании специализированных протоколов и программных средств шифрования данных;
- обучение студентов базовым принципам создания электронных подписей;
- овладение практическими навыками применения теоретических знаний для контроля целостности, шифрования конфиденциальной информации, решения задач идентификации и аутентификации;
- обучение применению криптографических методов защиты информации, порядку их ввода и вывода из эксплуатации, правилам эксплуатации.

2. Место дисциплины в структуре ОП специалитета

Дисциплина «Криптографические методы защиты информации» входит в перечень курсов базовой части ОП специальности «Информационно-аналитические системы безопасности».

Изучение дисциплины базируется на знаниях, полученных обучающимися при изучении дисциплин «Математический анализ» и «Теория вероятности и математическая статистика» а также на знаниях научных основ и закономерностей развития общества.

Кроме того, она имеет логические и содержательно-методические связи с дисциплинами по выбору базовой и вариативной частей ОП «Безопасность электронного документооборота», «Сети и системы передачи информации», «Безопасность операционных систем», «Безопасность информационно-аналитических систем», «Специальные технологии баз данных и информационных систем», «Математические методы в задачах финансового мониторинга».

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

В результате изучения учебной дисциплины у обучающегося формируются компетенции:

- способностью эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях (ПК-15).

В результате освоения дисциплины обучающийся должен:

Знать: основные понятия и определения, математические основы криптографии, историю криптографии и современные симметричные шифры, основы криптографии с открытым ключом, основные подходы к формированию цифровой подписи на основе различных алгоритмов с открытым ключом, управление ключами, модели шифров и математические методы их исследования

Уметь: пользоваться научно-технической литературой в области криптографии, применять отечественные и зарубежные стандарты в области криптографических методов защиты информации в процессе штатной эксплуатации специальных ИАС и средств обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстановления их работоспособности при внештатных ситуациях.

Владеть: навыками штатной эксплуатации специальных ИАС и средств обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстановления их работоспособности при внештатных ситуациях.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет **3 зачетные единицы (108 часов).**

4.1. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов/з.е.	Семестры			
		7			
Аудиторные занятия (всего)	**51/1,42**	**51/1,42**			
В том числе:					
Лекции (Л)	17/0,47	17/0,47			
Практические занятия (ПЗ)					
Семинары (С)					
Лабораторные работы (ЛР)	34/0,94	34/0,94			
Самостоятельная работа обучающихся (СРС) (всего)	**57/1,58**	**57/1,58**			
В том числе:					
Курсовой проект (работа)					
Расчетно-графические работы	27/0,75	27/0,75			
Реферат	30/0,83	30/0,83			
Другие виды СРС (если предусматриваются, приводится перечень видов СРС					
Форма промежуточной аттестации: Зачет с оценкой	+ 	+ 			
Общая трудоемкость	**108/3**	**108/3**			

5. Структура и содержание дисциплины

5.1. Структура дисциплины

№ п/п	Раздел дисциплины	Виды учебной работы, включая самостоятельную и трудоемкость (в часах)			
		Л	С/ПЗ	ЛР	СРС
1.	Введение. Основные понятия и определения.	2		4	5
2.	Математические основы криптографии	2		4	8
3.	Историческая криптография	2		4	6
4.	Современные симметричные шифры	2		4	8
5.	Криптография с открытым ключом	2		4	6
6.	Хеширование. Коды аутентичности сообщений. Электронная подпись.	2		4	6
7.	Управление ключами. Распределение симметричных ключей	2		4	8
8.	Разработка, производство, реализация и эксплуатация шифровальных (криптографических) средств защиты информации	3		6	10
9.	Промежуточная аттестация Зачет с оценкой				
	Итого:	**17**		**34**	**57**
	из них часов в интерактивной форме	**4**			

5.2. Содержание разделов дисциплины «Основы информационной безопасности», образовательные технологии

Лекционный курс

№ п/п	Наименование темы дисциплины	Трудоемкость (часы / зач. ед.)	Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
Тема 1.	Введение. Основные понятия и определения.	2/0,06	Предмет и задачи криптологии (криптографии и криптоанализа), формулируются основополагающие определения дисциплины	ПК-15	**Знать:** основные понятия и определения, математические основы криптографии, историю криптографии и современные симметричные шифры, основы криптографии с открытым ключом, основные подходы к формированию цифровой подписи на основе различных алгоритмов с открытым ключом, управление ключами, модели шифров и математические методы их исследования **Уметь:** пользоваться научно-технической литературой в области криптографии, применять отечественные и зарубежные стандарты в области криптографических методов защиты информации в процессе штатной эксплуатации специальных ИАС и средств обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстановления их работоспособности при внештатных ситуациях. **Владеть:** навыками штатной эксплуатации специальных ИАС и средств обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстановления их работоспособности при внештатных ситуациях.	Лекция-визуализация
Тема 2.	Математические основы криптографии	2/0,06	Алгебраические структуры. Группы. Кольца. Поля. Элементы теории чисел.			Лекция-визуализация
Тема 3.	Историческая криптография	2/0,06	Наиболее важные достижения криптографов в истории криптографии			Лекция-визуализация
Тема 4.	Современные симметричные шифры	2/0,06	Алгоритмы симметричного шифрования			Лекция-визуализация
Тема 5.	Криптография с открытым ключом	2/0,06	Алгоритмы асимметричного шифрования: RSA, алгоритм Диффи-Хеллмана, алгоритм Эль-Гамаля и др.			Лекция-визуализация
Тема 6	Хеширование Коды аутентичности сообщений. Электронная подпись.	2/0,06	Понятие хеш-функции, основные подходы к формированию цифровой подписи на основе отечественных и зарубежных стандартов.			Лекция-визуализация
Тема 7	Управление ключами. Распределение симметричных ключей.	2/0,06	Управление ключами. Распределение симметричных ключей. Удостоверяющий центр. PKI.			Лекция-визуализация
Тема 8	Разработка, производство, реализация и эксплуатация шифровальных (криптографических) средств защиты информации	3/0,08	Нормативно-правовое регулирование применения криптографических методов защиты информации			Лекция с разбором конкретных ситуаций
	Итого	**17/0,47**				

5.3. Практические и семинарские занятия, их наименование, содержание и объем в часах

№ п/п	№ раздела дисциплины	Наименование практических и семинарских занятий	Объем в часах / трудоемкость в з.е.

5.4 Лабораторные занятия, их наименование и объем в часах

№ п/п	№ раздела дисциплины	Наименование лабораторных работ	Объем в часах / трудоемкость в з.е.
1.	Введение. Основные понятия и определения.	Шифрованная файловая система Windows и Linux.	4/0,11
2.	Математические основы криптографии	Шифрование диска BitLocker в операционных системах Windows. Средство криптографической защиты информации SecretDisck.	4/0,11
3.	Историческая криптография	Основы криптоанализа симметричных шифров.	4/0,11
4.	Современные симметричные шифры	Аппаратно-программные комплексы шифрования (АПКШ Континент и др.).	4/0,11
5.	Криптография с открытым ключом	OpenSSL и LibreSSL. SSL-bump.	4/0,11
6.	Хеширование Коды аутентичности сообщений. Электронная подпись.	Криптопровайдеры (СКЗИ КриптоПро CSP и др.).	4/0,11
7.	Управление ключами. Распределение симметричных ключей.	Удостоверяющие центры (КриптоПро УЦ 2.0 и др.).	4/0,11
8.	Разработка, производство, реализация и эксплуатация шифровальных (криптографических) средств защиты информации	Подготовка пакета документов для лицензирования деятельности в области криптографической защиты информации и аккредитации удостоверяющего центра.	6/0,17
	Итого:		17/0,47
	из них часов в интерактивной форме		-

5.5. Примерная тематика курсовых проектов (работ)
Не предусмотрены.

5.6. Самостоятельная работа обучающихся

Содержание и объем самостоятельной работы обучающихся

№ п/п	Разделы и темы рабочей программы самостоятельного изучения	Перечень домашних заданий и других вопросов для самостоятельного изучения	Сроки выполнения	Объем в часах / трудоемкость в з.е.
1.	Введение. Основные понятия и определения.	Написание реферата	1-2 неделя	5/0,14
2.	Математические основы криптографии	Написание реферата	3-4 неделя	8/0,22
3.	Историческая криптография	Написание реферата	5-6 неделя	6/0,17
4.	Современные симметричные шифры	Написание реферата	7-8 неделя	8/0,22
5.	Криптография с открытым ключом	Написание реферата	9-10 неделя	6/0,17
6.	Хеширование. Коды аутентичности сообщений. Электронная подпись.	Написание реферата	11-12 неделя	8/0,22
7.	Управление ключами. Распределение симметричных ключей		13-14 неделя	8/0,22
8.	Разработка, производство, реализация и эксплуатация шифровальных (криптографических) средств защиты информации	Написание реферата	15-16 неделя	10/0,28
	Итого			**57/1,58**

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

6.1. Методические указания (собственные разработки)

6.2 Литература для самостоятельной работы

1. Бабаш, А.В. Криптографические методы защиты информации. Т. 3 [Электронный ресурс]: учебно-методическое пособие / А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2014. - 216 с. - ЭБС «Znanium. com» - Режим доступа: http://znanium.com/catalog.php?bookinfo=432654.
2. Басалова, Г.В. Основы криптографии [Электронный ресурс]/ Басалова Г.В. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 282 с. - ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/52158
3. Калмыков, И.А. Криптографические методы защиты информации [Электронный ресурс]: лабораторный практикум/ И.А. Калмыков, Д.О. Науменко, Т.А. Гиш. - Ставрополь: Северо-Кавказский федеральный университет, 2015. - 109 с. - ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/63099.html .
4. Лапонина, О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс]: учебное пособие/ О.Р. Лапонина. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 242 с. - ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/52217.html.
5. Ларин, Д.А. . Криптографическая деятельность в России от Полтавы до Бородина [Электронный ресурс]: монография/ Д.А, Ларин. - Москва: РИОР: ИНФРА-М, 2015. - 282 с. - ЭБС «Znanium. com» - Режим доступа:

http://znanium.com/catalog.php?bookinfo=479196.html.

6. Ожиганов, А.А. Криптографические системы с секретным и открытым ключом [Электронный ресурс]: учебное пособие/ А.А. Ожиганов. - СПб.: Университет ИТМО, 2015. - 66 с. - ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/67230.html

7. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс]/ А.А. Петров. - Саратов: Профобразование, 2017. - 446 с. - ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/63800.html

8. Практикум по выполнению лабораторных работ по дисциплине Криптографические методы защиты информации [Электронный ресурс]/ [сост. Смирнов А.Э., Пономарёва Ю.А.]. - М.: Московский технический университет связи и информатики, 2015. - 67 с. - ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/61738.html .

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Этапы формирования компетенции (номер семестра согласно учебному плану)	**Наименование учебных дисциплин, формирующих компетенции в процессе освоения образовательной программы**
ПК-15: способностью эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях	
5,6	Специальные технологии баз данных и информационных систем
7	Криптографические методы защиты информации
8	Безопасность электронного документооборота
10	Математические методы в задачах финансового мониторинга

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
ПК-5: способность проводить обоснование и выбор оптимального решения задач в сфере профессиональной деятельности					
Знать: основные понятия и определения, математические основы криптографии, историю криптографии и современные симметричные шифры, основы криптографии с открытым ключом, основные подходы к формированию цифровой подписи на основе различных алгоритмов с открытым ключом, управление ключами, модели шифров и математические методы их исследования.	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	тесты, рефераты, зачет
Уметь: пользоваться научно-технической литературой в области криптографии, применять отечественные и зарубежные стандарты в области криптографических методов защиты информации в процессе штатной эксплуатации специальных ИАС и средств обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстановления их работоспособности при внештатных ситуациях.	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: навыками штатной эксплуатации специальных ИАС и средств обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстановления их работоспособности при внештатных ситуациях.	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

7.3. Типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Тестовые задания для текущего контроля знаний по дисциплине

Вариант № 1

< Вопрос № 1 >

Электронная подпись бывает:

- Созданная ввиде отдельного файла
- Присоединенной к файлу
- Созданная ввиде атрибутов к файлу

< Вопрос № 2 >

Процесс зашифрования или расшифрования называется:

- Шифровка
- Шифрование

< Вопрос № 3 >

Преобразование текста с целью скрыть его содержание от НСД -

- Шифрование
- Хеширование

< Вопрос № 4 >

Как называется криптографический метод который представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста?

- аналитическое преобразование
- комбинированное преобразование

< Вопрос № 5 >

Американский учёный-теоретик в области компьютерных наук, профессор компьютерных наук и молекулярной биологии в Университете Южной Калифорнии, известный как соавтор системы шифрования RSA (Rivest — Shamir — Adleman, 1977 год) и ДНК-вычислений:

- Ади Шамир
- Рональд Линн Ривест
- Леонард Макс Адлеман

< Вопрос № 6 >

Одна из первых книг по шифровке написана -

- аббатом Трителлием (1462-1516) из Германии
- аббатом Трителлием (1416-1466) из Италии

< Вопрос № 7 >

Для каких целей в криптографии используются хэш-функция:

- создания образов некоторых данных для их безопасного хранения
- расчета контрольной суммы пакета
- образования так называемых дайджестов h(m) для сообщений m

< Вопрос № 8 >

Как называется криптографический метод суть которого заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа?

- кодирование
- имитовставка
- метод псевдослучайного ряда
- гаммирование

< Вопрос № 9 >

При использовании усиленных электронных подписей участники электронного взаимодействия обязаны:

- обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия
- не использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным Федеральным законом "Об электронной подписи"
- уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении
- использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена

< Вопрос № 10 >

PKI это:

- Инфраструктура открытых ключей (PKI - Public Key Infrastructure)
- Инфраструктура закрытых ключей (PKI - Private Key Infrastructure)

< Вопрос № 11 >

Преобразование по детерминированному алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины:

- хеширование
- хэширование
- кэширование
- кеширование

< Вопрос № 12 >

Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- ключа проверки электронной подписи может не создаваться
- для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом
- ключ проверки электронной подписи указан в квалифицированном сертификате

< Вопрос № 13 >

Меры защиты от негативного влияния аппаратного окружения на СКЗИ^

- Физические лица допускаются к работе с СКЗИ согласно перечню пользователей СКЗИ, утверждаемому соответствующим обладателем конфиденциальной информации
- Проведение при необходимости специальных проверок и анализ активной составляющей аппаратной части, на которой функционируют СКЗИ
- Проверка ПО на соответствие требованиям к ПО ФСБ России и требованиям нормативных правовых актов и методических документов ФСТЭК России
- Контроль целостности программных модулей

< Вопрос № 14 >

Чтобы гарантировать надежную защиту информации, к системам с открытым ключом предъявляются два важных и очевидных требования:

- Преобразование исходного текста должно быть обратимым и гарантировать его восстановление на основе открытого ключа.
- Определение закрытого ключа на основе открытого также должно быть возможным на современном технологическом уровне. При этом не желательна точная нижняя оценка сложности (количества операций) раскрытия шифра.
- Преобразование исходного текста должно быть необратимым и исключать его восстановление на основе открытого ключа.
- Определение закрытого ключа на основе открытого также должно быть невозможным на современном технологическом уровне. При этом желательна точная нижняя оценка сложности (количества операций) раскрытия шифра.

< Вопрос № 15 >

Квалифицированная электронная подпись признается действительной до тех пор, пока решением суда не установлено иное, при одновременном соблюдении следующих условий:

•квалифицированная электронная подпись используется с учетом ограничений, содержащихся в квалифицированном сертификате лица, подписывающего электронный документ (если такие ограничения установлены)

•квалифицированный сертификат создан и выдан аккредитованным удостоверяющим центром, аккредитация которого действительна на день выдачи указанного сертификата

•квалифицированный сертификат действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен

•квалифицированный сертификат не действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен

•имеется положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания

< Вопрос № 16 >

С помощью чего можно преобразовать (по определённому алгоритму) входной массив данных произвольной длины в выходную битовую строку фиксированной длины -

- хэш-код
- хэш-функция

< Вопрос № 17 >

Один из самых известных американских криптографов, заслуживший мировую известность за

концепцию криптографии с открытым ключом:

- Леонард Макс Адлеман
- Клод Шеннон
- Уитфилд Диффи
- А.Конан Дойл

< Вопрос № 18 >

Согласно Федеральному закону от 4 мая 2011 г. N 99-ФЗ "О лицензировании отдельных видов деятельности" к видам деятельности, на которые требуются лицензии, относятся:

- Предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей.
- Применение средств шифрования

< Вопрос № 19 >

При обращении в аккредитованный удостоверяющий центр заявитель указывает на ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются) и представляет следующие документы, подтверждающие достоверность информации, предоставленной заявителем для включения в квалифицированный сертификат, либо их надлежащим образом заверенные копии:

- водительское удостоверение
- основной документ, удостоверяющий личность, страховое свидетельство государственного пенсионного страхования заявителя - физического лица или учредительные документы, документ, подтверждающий факт внесения записи о юридическом лице в Единый государственный реестр юридических лиц, и свидетельство о постановке на учет в налоговом органе заявителя - юридического лица
- доверенность или иной документ, подтверждающий право заявителя действовать от имени других лиц
- надлежащим образом заверенный перевод на русский язык документов о государственной регистрации юридического лица в соответствии с законодательством иностранного государства (для иностранных юридических лиц)

< Вопрос № 20 >

Как называется принцип построения криптографических алгоритмов, согласно которому в секрете держится только определенный набор их параметров (ключ), а все остальное может быть открытым без снижения стойкости алгоритма ниже допустимой величины?

- Принцип Кирхгофа
- Протокол криптографический

< Вопрос № 21 >

Как называется набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах?

- Протокол криптографический
- Принцип Кирхгофа

< Вопрос № 22 >

Допускается не указывать в качестве владельца сертификата ключа проверки электронной подписи -

- директоров атомных электростанций
- в случаях, предусмотренных федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами
- в сертификате ключа проверки электронной подписи, используемом для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций
- физическое лицо, действующее от имени юридического лица

< Вопрос № 23 >

Обеспечение доверия к участникам процессов обработки данных включает в себя:

- Экспертной оценкой безопасности зафиксированных средств обработки и отображения.
- Физические лица допускаются к работе с СКЗИ согласно перечню пользователей СКЗИ, утверждаемому соответствующим обладателем конфиденциальной информации.
- Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения.
- Наличие в ОРГАНИЗАЦИИ должного уровня исполнительской дисциплины

< Вопрос № 24 >

Какие из перечисленных алгоритмов имеют более высокую производительность?

- Алгоритмы с симметричными ключами
- Алгоритмы с асимметричными ключами

< Вопрос № 25 >

Каждый орган криптографической защиты для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей должен иметь

- необходимое число надежных металлических хранилищ, оборудованных внутренними замками с одним экземпляром ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин
- необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин
- необходимое число надежных металлических хранилищ, оборудованных нависными замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин

< Вопрос № 26 >

Аккредитованный удостоверяющий центр обязан хранить в течение срока его деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федераци, следующую информацию:

- реквизиты всех документов, удостоверяющего личность владельца квалифицированного сертификата - физического лица
- сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата
- реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица
- сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат

< Вопрос № 27 >

Как называется криптографический метод заключающийся в том, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее определенным правилом?

- перестановка
- подстановка

< Вопрос № 28 >

Доверие к средствам криптографической защиты не предполагает комплексное решение следующих подзадач:

- Оценка реализации соответствующего уровня контроля присутствия НДВ
- Оценка влияния программно-аппаратного окружения на корректность работы СКЗИ
- Доказательство корректности и безопасности целевых функций СКЗИ (формирование защищаемых объектов, отсутствие утечек ключевой информации и т.д.)
- Оценка корректности встраивания криптографических сервисов в прикладное ПО на основе согласованных с ФСБ рекомендаций

< Вопрос № 29 >

Удостоверяющий центр:

- выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем
- создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям)
- аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей
- устанавливает сроки действия сертификатов ключей проверки электронных подписей

< Вопрос № 30 >

Видами электронных подписей, , являются:

- усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись
- простая электронная подпись и усиленная электронная подпись
- простая подпись и усиленная подпсиь
- неквалифицированная электронная подпись и квалифицированная электронная подпись

< Вопрос № 31 >

Основным достоинством криптографических методов защиты информации является то, что они:

- обеспечивают высокую гарантированную стойкость защиты, которую можно рассчитать и выразить в числовой форме (средним числом операций или временем, необходимым для раскрытия зашифрованной информации или вычисления ключей)
- обеспечивают высокую гарантированную стойкость защиты, которую не возможно рассчитать и выразить в числовой форме (например, средним числом операций или временем, необходимым для раскрытия зашифрованной информации или вычисления ключей)

< Вопрос № 32 >

Удостоверяющий центр:

- проверяет уникальность ключей проверки электронных подписей в регистре сертификатов
- создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей
- устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет"
- ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных п

< Вопрос № 33 >

Доверие к средствам криптографической защиты предполагает комплексное решение следующих подзадач:

- Оценка ПО не взаимодействующего с криптографическими сервисами
- Анализ комплекса организационно-технических мер защиты, обеспечивающих заданный уровень криптографической защиты
- Исследование криптографических алгоритмов и их реализации
- Оценка криптографических сервисов

< Вопрос № 34 >

Как называется защита информационных процессов от целенаправленных попыток отклонить их от нормальных условий протекания, базирующаяся на криптографических преобразованиях данны?

- Криптографическая защита
- Криптование

< Вопрос № 35 >

Информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается

- равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью
- электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия

< Вопрос № 36 >

По окончании рабочего дня спецпомещения органа криптографической защиты и установленные в них хранилища:

- печати, предназначенные для опечатывания хранилищ, не должны находиться у сотрудников органа криптографической защиты, ответственных за эти хранилища
- ключи от хранилищ должны быть сданы под расписку в соответствующем журнале руководителю органа криптографической защиты или лицу, им уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище
- ключи от спецпомещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ органа криптографической защиты, в опечатанном виде должны быть

сданы под расписку в соответствующем журнале службе охраны или дежурному по организации одновременно с передачей под охрану самих спецпомещений
- должны быть закрыты, хранилища опечатаны

< Вопрос № 37 >

Устойчивость криптографического алгоритма к его криптоанализу называется:

- Криптостойкость
- Криптостойкая гамма
- Криптографическая стойкость

< Вопрос № 38 >

Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, обладатели которой не имеют лицензий ФСБ России, лицензиаты организуют и обеспечивают либо по указанию вышестоящей организации, либо на основании договоров на оказание услуг по криптографической защите конфиденциальной информации:

- при этом лицензиаты ФСБ России должны обеспечивать комплексность защиты конфиденциальной информации, в том числе посредством применения некриптографических средств защиты
- при этом лицензиаты ФСБ России не должны обеспечивать комплексность защиты конфиденциальной информации, в том числе посредством применения некриптографических средств защиты

< Вопрос № 39 >

Размещение, специальное оборудование, охрана и организация режима в спецпомещениях органов криптографической защиты должны исключить:

- возможность пребывания в них пользователей СКЗИ
- возможность неконтролируемого проникновения или пребывания в них посторонних лиц
- возможность просмотра посторонними лицами ведущихся там работ

< Вопрос № 40 >

Одной электронной подписью могут быть подписаны

- только один электронный документ
- несколько связанных между собой электронных документов (пакет электронных документов)

< Вопрос № 41 >

Раунд это

- Один шаг шифрования в шифре Файстеля и близких ему по архитектуре шифрах, в ходе которого одна или несколько частей шифруемого блока данных подвергается модификации.
- Секретный элемент, получаемый из ключа криптоалгоритма, и используемый шифром Файстеля и аналогичными криптоалгоритмами на одном раунде шифрования.

< Вопрос № 42 >

Назовите одну из причин популярности RSA?

- Возможность гарантированно оценить защищенность
- Высокая по сравнению с симметричными системами производительность

< Вопрос № 43 >

Если аппаратные или аппаратно - программные СКЗИ подключаются к системной шине или к

одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно

- пользователями СКЗИ
- с соответствующими аппаратными средствами

Предмет: "Криптография"
Тема: "Учебный тест"
Вариант № 2

< Вопрос № 1 >
Если аппаратные или аппаратно - программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно

- с соответствующими аппаратными средствами
- пользователями СКЗИ

< Вопрос № 2 >
Как называется принцип построения криптографических алгоритмов, согласно которому в секрете держится только определенный набор их параметров (ключ), а все остальное может быть открытым без снижения стойкости алгоритма ниже допустимой величины?

- Принцип Кирхгофа
- Протокол криптографический

< Вопрос № 3 >
Обязанности сотрудников органов криптографической защиты должны учитывать, что безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации обеспечивается:

- своевременным выявлением сотрудниками органов криптографической защиты попыток посторонних лиц получить сведения о не защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых документах к ним
- надежным хранением сотрудниками органов криптографической защиты СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, носителей конфиденциальной информации
- соблюдением сотрудниками органов криптографической защиты режима конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним
- немедленным принятием сотрудниками органов криптографической защиты мер по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.
- точным выполнением сотрудниками органов криптографической защиты требований к обеспечению безопасности конфиденциальной информации

< Вопрос № 4 >
При использовании каких алгоритмов требуются более надежные (высоконадежные) механизмы для распределения ключей?

- Алгоритмы с симметричными ключами, так как для шифрования и расшифрования используется один и тот же ключ

- Алгоритмы с асимметричными ключами

< Вопрос № 5 >

Раундовый ключ это:

- Секретный элемент, получаемый из ключа криптоалгоритма, и используемый шифром Файстеля и аналогичными криптоалгоритмами на одном раунде шифрования.
- Один шаг шифрования в шифре Файстеля и близких ему по архитектуре шифрах, в ходе которого одна или несколько частей шифруемого блока данных подвергается модификации.

< Вопрос № 6 >

Лицензионные требования при осуществлении деятельности, связанной с криптографической защитой информации:

- наличие у соискателя лицензии (лицензиата) условий для соблюдения конфиденциальности информации, необходимых для выполнения работ и оказания услуг, составляющих лицензируемую деятельность, в соответствии с требованиями о соблюдении конфиденциальности информации, установленными Федеральным законом "Об информации, информационных технологиях и о защите информации"
- наличие в штате у соискателя лицензии (лицензиата) квалифицированного персонала
- использование соискателем лицензии (лицензиатом) предназначенных для осуществления лицензируемой деятельности программ для электронных вычислительных машин и баз данных, принадлежащих соискателю лицензии (лицензиату) на праве собственности или ином законном основании
- наличие у соискателя лицензии (лицензиата) права собственности или иного законного основания на владение и использование помещений, сооружений, технологического, испытательного, контрольно-измерительного оборудования и иных объектов, необходимых для осуществления лицензируемой деятельности

< Вопрос № 7 >

Единицей поэкземплярного учета ключевых документов считается:

- ключевой носитель однократного использования
- ключевой носитель многократного использования

< Вопрос № 8 >

Как называется раздел криптографии, изучающий и разрабатывающий асимметричные криптографические системы?

- "Современная" криптография
- Традиционная криптография

< Вопрос № 9 >

Секретный ключ это

- Набор секретных параметров одного из алгоритмов асимметричной криптосистемы.
- Свойство данных быть известными и доступными только тому кругу субъектов, которому для которого они предназначены и свойство криптосистемы обеспечивать секретность защищаемых данных.

< Вопрос № 10 >

Для разработки и осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ конфиденциальной информации лицензиат ФСБ России создает один или несколько:

- секретных ключей
- органов криптографической защиты

< Вопрос № 11 >

Согласно Федеральному закону от 4 мая 2011 г. N 99-ФЗ "О лицензировании отдельных видов деятельности" к видам деятельности, на которые требуются лицензии, относятся:

- Применение средств шифрования
- Предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей.

< Вопрос № 12 >

Шифр, в котором знание шифртекста не позволяет улучшить оценку соответствующего открытого текста называется:

- Шифр абсолютно стойкий
- Шифр несовершенный

< Вопрос № 13 >

Массив зашифрованных данных, то есть данных, подвергнутых процедуре зашифрования:

- Шифртекст
- Шифровка
- Шифротекст

< Вопрос № 14 >

Безопасность хранения и обработки с использованием СКЗИ конфиденциальной информации, передаваемой вне сетей конфиденциальной связи, организуют и обеспечивают лица, имеющие

- лицензию ФСТЭК России
- лицензию ФСБ России

< Вопрос № 15 >

Какие из перечисленных алгоритмов имеют более высокую производительность?

- Алгоритмы с симметричными ключами
- Алгоритмы с асимметричными ключами

< Вопрос № 16 >

Совокупность алгоритмов криптографических преобразований, отображающих множество возможных открытых данных на множество возможных зашифрованных данных, и обратных им преобразований называется:

- шифр
- хэш
- ключ

< Вопрос № 17 >

Какой документ установил основные правила проведения сертификационных исследований и испытаний криптографических средств защиты информации и закрытых с их помощью систем и комплексов обработки, хранения и передачи информации?

- РОСС RU.0003.030003

- РОСС RU.0001.030001
- РОСС RU.0001.030003

< Вопрос № 18 >

Процесс зашифрования или расшифрования называется:

- Шифровка
- Шифрование

< Вопрос № 19 >

Как называется шифр в котором отдельные символы исходного текста или их группы заменяются на другие символы или группы символов, сохраняя при этом свое положение в тексте относительно других заменяемых групп?

- шифр замены
- шифр перестановки

< Вопрос № 20 >

Как называется криптографический метод который представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста?

- аналитическое преобразование
- комбинированное преобразование

< Вопрос № 21 >

Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

- Утверждена Приказом ФАПСИ при Президенте РФ от 13.06.2001 № 152
- Утверждена Приказом ФАПСИ при Президенте РФ от 13.06.2001 № 153
- Утверждена Приказом ФАПСИ при Президенте РФ от 13.06.2001 № 151

< Вопрос № 22 >

Основные задачи системы информационной безопасности, которые решает PKI:

- обеспечение аутентификации пользователей и ресурсов, к которым обращаются пользователи
- обеспечение целостности информации
- исключить возможность подтверждения совершенных пользователями действий с информацией
- обеспечение конфиденциальности информации

< Вопрос № 23 >

Как называется шифр, составленный из нескольких более простых шифров, которые используются в определенной последовательности при зашифровании и расшифровании данных:

- Шифр составной
- Шифр комбинированный

< Вопрос № 24 >

Для каких целей в криптографии используются хэш-функция:

- создания образов некоторых данных для их безопасного хранения

- образования так называемых дайджестов h(m) для сообщений m
- расчета контрольной суммы пакета

< Вопрос № 25 >

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" регулирует отношения в области использования:

- в любом случае
- электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий

< Вопрос № 26 >

Как называется функция, переводящая произвольную конечную бинарную последовательность в последовательность определенной длины?

- Кеш-функция
- Хеш-функция
- Кэш-функция
- Хэш-функция

< Вопрос № 27 >

PKI это:

- Инфраструктура открытых ключей (PKI - Public Key Infrastructure)
- Инфраструктура закрытых ключей (PKI - Private Key Infrastructure)

< Вопрос № 28 >

ПКЗ-2005 необходимо руководствоваться при разработке, производстве, реализации и эксплуатации средств криптографической защиты информации конфиденциального характера в следующих случаях:

- при организации криптографической защиты информации конфиденциального характера в организациях независимо от их организационно-правовой формы и формы собственности при выполнении ими заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд
- если информация конфиденциального характера не подлежит защите в соответствии с законодательством Российской Федерации
- если обязательность защиты информации конфиденциального характера возлагается законодательством Российской Федерации на лиц, имеющих доступ к этой информации или наделенных полномочиями по распоряжению сведениями, содержащимися в данной информации
- при организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации

< Вопрос № 29 >

Что скрывает факт передачи информации -

- Криптография
- Стеганография

< Вопрос № 30 >

Меры защиты от негативного влияния аппаратного окружения на СКЗИ^

- Контроль целостности программных модулей
- Проведение при необходимости специальных проверок и анализ активной составляющей аппаратной части, на которой функционируют СКЗИ
- Физические лица допускаются к работе с СКЗИ согласно перечню пользователей СКЗИ, утверждаемому соответствующим обладателем конфиденциальной информации
- Проверка ПО на соответствие требованиям к ПО ФСБ России и требованиям нормативных правовых актов и методических документов ФСТЭК России

< Вопрос № 31 >

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

- соблюдение конфиденциальности информации ограниченного доступа
- реализацию права на доступ к информации
- своевременное обнаружение фактов несанкционированного доступа к информаци
- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации

< Вопрос № 32 >

Если в использовании СКЗИ выявлены серьезные нарушения, из-за чего становится реальной утечка конфиденциальной информации, безопасность которой обеспечивается с использованием СКЗИ, то лицензиаты ФСБ России

- вправе дать указание о немедленном прекращении использования СКЗИ до устранения причин выявленных нарушений
- вправе дать указание о прекращении использования СКЗИ навсегда

< Вопрос № 33 >

С помощью чего можно преобразовать (по определённому алгоритму) входной массив данных произвольной длины в выходную битовую строку фиксированной длины -

- хэш-функция
- хэш-код

< Вопрос № 34 >

Преобразование текста с целью скрыть его содержание от НСД -

- Хеширование
- Шифрование

< Вопрос № 35 >

Решения CSP VPN обеспечивают построение виртуальных защищенных сетей (VPN) предприятия:

- Контроль доступа на уровне хостов, индивидуальных пользователей и отдельных приложений
- Шифрование (конфиденциальность), электронно-цифровая подпись (целостность, аутентификация) IP пакетов гибкость в реализации политики сетевой защиты (множественность алгоритмов шифрования, включая ГОСТ; сложные конфигурации туннелей); высокая стойкость защиты информации.
- Формирование защищенных соединений междуподсетями, компьютерами (клиент-сервер, одноранговые клиенты).
- Аутентификация узлов сети и аутентификация пользователей.

< Вопрос № 36 >

Обеспечение доверия к участникам процессов обработки данных включает в себя:

- Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения.
- Экспертной оценкой безопасности зафиксированных средств обработки и отображения.
- Наличие в ОРГАНИЗАЦИИ должного уровня исполнительской дисциплины
- Физические лица допускаются к работе с СКЗИ согласно перечню пользователей СКЗИ, утверждаемому соответствующим обладателем конфиденциальной информации.

< Вопрос № 37 >

Не существует Криптосистем -

- Симметричные
- Параллельные
- Ассиметричные

< Вопрос № 38 >

Электронная подпись бывает:

- Созданная ввиде отдельного файла
- Присоединенной к файлу
- Созданная ввиде атрибутов к файлу

< Вопрос № 39 >

При использовании усиленных электронных подписей участники электронного взаимодействия обязаны:

- не использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным Федеральным законом "Об электронной подписи"
- уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении
- использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена
- обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия

< Вопрос № 40 >

Доверие к средствам криптографической защиты не предполагает комплексное решение следующих подзадач:

- Оценка корректности встраивания криптографических сервисов в прикладное ПО на основе согласованных с ФСБ рекомендаций
- Оценка влияния программно-аппаратного окружения на корректность работы СКЗИ
- Оценка реализации соответствующего уровня контроля присутствия НДВ
- Доказательство корректности и безопасности целевых функций СКЗИ (формирование защищаемых объектов, отсутствие утечек ключевой информации и т.д.)

< Вопрос № 41 >

Доверие к средствам криптографической защиты предполагает комплексное решение следующих подзадач:

- Анализ комплекса организационно-технических мер защиты, обеспечивающих заданный уровень криптографической защиты
- Оценка ПО не взаимодействующего с криптографическими сервисами
- Оценка криптографических сервисов
- Исследование криптографических алгоритмов и их реализации

< Вопрос № 42 >

Каждый орган криптографической защиты для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей должен иметь

- необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин
- необходимое число надежных металлических хранилищ, оборудованных внутренними замками с одним экземпляром ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин
- необходимое число надежных металлических хранилищ, оборудованных нависными замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин

< Вопрос № 43 >

Одна из первых книг по шифровке написана -

- аббатом Трителлием (1462-1516) из Германии
- аббатом Трителлием (1416-1466) из Италии

Предмет: "Криптография"

Тема: "Учебный тест"

Вариант № 3

< Вопрос № 1 >

Американский специалист по криптографии, имеет звание Профессора имени Эндрю и Эрны Витерби по компьютерным наукам на Факультете электротехники и компьютерных наук (EECS) и состоит в штате кафедры CSAIL в Массачусетском технологическом институте, также является членом лаборатории Теория вычислений и лидером группы Криптография и информационная безопасность?

- Рональд Линн Ривест
- Леонард Макс Адлеман
- Ади Шамир

< Вопрос № 2 >

Доверие к средствам криптографической защиты предполагает комплексное решение следующих подзадач:

- Анализ комплекса организационно-технических мер защиты, обеспечивающих заданный уровень криптографической защиты
- Оценка ПО не взаимодействующего с криптографическими сервисами
- Исследование криптографических алгоритмов и их реализации
- Оценка криптографических сервисов

< Вопрос № 3 >

При использовании усиленных электронных подписей участники электронного взаимодействия обязаны:

- обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия
- использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена
- не использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным Федеральным законом "Об электронной подписи"
- уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении

< Вопрос № 4 >

Преобразование по детерминированному алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины:

- хеширование
- кеширование
- кэширование
- хэширование

< Вопрос № 5 >

Рассеивание это

- Распространение влияния одного знака открытого текста на много знаков шифртекста, а также распространение влияния одного элемента ключа на много знаков шифртекста.
- Преобразование исходных данных перед или во время зашифрования с использованием псевдослучайной последовательности данных, имеющее целью скрыть наличие в них регулярностей различного типа, например - наличие идентичных блоков.

< Вопрос № 6 >

Видами электронных подписей, , являются:

- простая подпись и усиленная подпсиь
- неквалифицированная электронная подпись и квалифицированная электронная подпись
- усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись
- простая электронная подпись и усиленная электронная подпись

< Вопрос № 7 >

Специалист в области криптографии это

- Криптоаналитик
- Криптограф

< Вопрос № 8 >

Криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований:

- Вычисление логарифма в конечном поле
- Перестановки таблиц кодировки
- Разложение больших чисел на простые множители
- Вычисление корней алгебраических уравнений

< Вопрос № 9 >

Первый алгоритм асимметричного шифрования -

- RSA
- RC
- IDEA
- DES

< Вопрос № 10 >

Квалифицированная электронная подпись признается действительной до тех пор, пока решением суда не установлено иное, при одновременном соблюдении следующих условий:

- квалифицированная электронная подпись используется с учетом ограничений, содержащихся в квалифицированном сертификате лица, подписывающего электронный документ (если такие ограничения установлены)
- квалифицированный сертификат не действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен
- квалифицированный сертификат действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен
- имеется положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания
- квалифицированный сертификат создан и выдан аккредитованным удостоверяющим центром, аккредитация которого действительна на день выдачи указанного сертификата

< Вопрос № 11 >

Один из самых известных американских криптографов, заслуживший мировую известность за концепцию криптографии с открытым ключом:

- Леонард Макс Адлеман
- Клод Шеннон
- Уитфилд Диффи
- А.Конан Дойл

< Вопрос № 12 >

При обращении в аккредитованный удостоверяющий центр заявитель указывает на ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются) и представляет следующие документы, подтверждающие достоверность информации, предоставленной заявителем для включения в квалифицированный сертификат, либо их надлежащим образом заверенные копии:

- водительское удостоверение
- доверенность или иной документ, подтверждающий право заявителя действовать от имени других лиц
- основной документ, удостоверяющий личность, страховое свидетельство государственного пенсионного страхования заявителя - физического лица или учредительные документы, документ, подтверждающий факт внесения записи о юридическом лице в Единый государственный реестр юридических лиц, и свидетельство о постановке на учет в налоговом органе заявителя - юридического лица
- надлежащим образом заверенный перевод на русский язык документов о государственной

регистрации юридического лица в соответствии с законодательством иностранного государства (для иностранных юридических лиц)

< Вопрос № 13 >

Одной электронной подписью могут быть подписаны

- только один электронный документ
- несколько связанных между собой электронных документов (пакет электронных документов)

< Вопрос № 14 >

Один из самых известных американских криптографов, который получил известность благодаря разработке первой асимметричной криптосистемы в соавторстве с Уитфилдом Диффи и Ральфом Мерклем (1952г)?

- Рональд Линн Ривест
- Леонард Макс Адлеман
- Уитфилд Диффи
- Ади Шамир

< Вопрос № 15 >

Раунд это

- Один шаг шифрования в шифре Файстеля и близких ему по архитектуре шифрах, в ходе которого одна или несколько частей шифруемого блока данных подвергается модификации.
- Секретный элемент, получаемый из ключа криптоалгоритма, и используемый шифром Файстеля и аналогичными криптоалгоритмами на одном раунде шифрования.

< Вопрос № 16 >

Допускается не указывать в качестве владельца сертификата ключа проверки электронной подписи -

- директоров атомных электростанций
- в случаях, предусмотренных федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами
- физическое лицо, действующее от имени юридического лица
- в сертификате ключа проверки электронной подписи, используемом для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций

< Вопрос № 17 >

Безопасность хранения и обработки с использованием СКЗИ конфиденциальной информации, передаваемой вне сетей конфиденциальной связи, организуют и обеспечивают лица, имеющие

- лицензию ФСБ России
- лицензию ФСТЭК России

< Вопрос № 18 >

Какие из перечисленных алгоритмов имеют более высокую производительность?

- Алгоритмы с симметричными ключами
- Алгоритмы с асимметричными ключами

< Вопрос № 19 >

Если в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота документ должен быть заверен печатью, электронный документ, подписанный усиленной электронной подписью, признается

- документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия
- равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью

< Вопрос № 20 >

Аккредитованный удостоверяющий центр обязан хранить в течение срока его деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федераци, следующую информацию:

- реквизиты всех документов, удостоверяющего личность владельца квалифицированного сертификата - физического лица
- сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата
- сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат
- реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица

< Вопрос № 21 >

Как называется криптографический метод заключающийся в том, что символы шифруемого текста переставляются по некоторому правилу в пределах заданного блока передаваемого текста?

- перестановка
- подстановка

< Вопрос № 22 >

Лицензионные требования при осуществлении деятельности, связанной с криптографической защитой информации:

- использование соискателем лицензии (лицензиатом) предназначенных для осуществления лицензируемой деятельности программ для электронных вычислительных машин и баз данных, принадлежащих соискателю лицензии (лицензиату) на праве собственности или ином законном основании
- наличие у соискателя лицензии (лицензиата) права собственности или иного законного основания на владение и использование помещений, сооружений, технологического, испытательного, контрольно-измерительного оборудования и иных объектов, необходимых для осуществления лицензируемой деятельности
- наличие в штате у соискателя лицензии (лицензиата) квалифицированного персонала
- наличие у соискателя лицензии (лицензиата) условий для соблюдения конфиденциальности информации, необходимых для выполнения работ и оказания услуг, составляющих лицензируемую деятельность, в соответствии с требованиями о соблюдении конфиденциальности информации, установленными Федеральным законом "Об информации, информационных технологиях и о защите информации"

< Вопрос № 23 >

Информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается

- равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью
- электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия

< Вопрос № 24 >

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, не обязаны обеспечить:

- постоянный контроль за обеспечением уровня защищенности информации
- невозможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации

< Вопрос № 25 >

Основным достоинством криптографических методов защиты информации является то, что они:

- обеспечивают высокую гарантированную стойкость защиты, которую можно рассчитать и выразить в числовой форме (средним числом операций или временем, необходимым для раскрытия зашифрованной информации или вычисления ключей)
- обеспечивают высокую гарантированную стойкость защиты, которую не возможно рассчитать и выразить в числовой форме (например, средним числом операций или временем, необходимым для раскрытия зашифрованной информации или вычисления ключей)

< Вопрос № 26 >

СКЗИ это:

- средство комплексной защиты информации
- система криптографической защиты информации
- средства криптографической защиты информации

< Вопрос № 27 >

Удостоверяющий центр:

- проверяет уникальность ключей проверки электронных подписей в регистре сертификатов
- создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей
- ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных п
- устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированны-

ми, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет"

< Вопрос № 28 >

Код аутентификации это:

- Имитовставка, код фиксированной длины, вырабатываемый из данных с использованием секретного ключа и добавляемый к данным с целью обнаружения факта изменений хранимых или передаваемых по каналу связи данных.
- Код фиксированной длины, вырабатываемый из данных с использованием вычислительно необратимой функции с целью обнаружения факта изменений хранимых или передаваемых по каналу связи данных.

< Вопрос № 29 >

Массив зашифрованных данных, то есть данных, подвергнутых процедуре зашифрования:

- Шифротекст
- Шифртекст
- Шифровка

< Вопрос № 30 >

По окончании рабочего дня спецпомещения органа криптографической защиты и установленные в них хранилища:

- печати, предназначенные для опечатывания хранилищ, не должны находиться у сотрудников органа криптографической защиты, ответственных за эти хранилища
- ключи от хранилищ должны быть сданы под расписку в соответствующем журнале руководителю органа криптографической защиты или лицу, им уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище
- должны быть закрыты, хранилища опечатаны
- ключи от спецпомещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ органа криптографической защиты, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службе охраны или дежурному по организации одновременно с передачей под охрану самих спецпомещений

< Вопрос № 31 >

Как называется криптографический метод который представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста?

- комбинированное преобразование
- аналитическое преобразование

< Вопрос № 32 >

Лицензирование деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, осуществляет:

- ФСТЭК России
- Минкомсвязь
- ФСБ России

< Вопрос № 33 >

Как называется архитектура построения блочных шифров, доминирующая в настоящее время в традиционной криптографии, в которой весь процесс шифрования блока выполняется за серию шагов (раундов), на каждом из которых блок делится на изменяемую и постоянную части, с помощью функции шифрования из постоянной части и раундового ключа вырабатывается модифицирующий код, который используется для модификации?

- Традиционная архитектура
- Сеть Файстеля

< Вопрос № 34 >

Размещение, специальное оборудование, охрана и организация режима в спецпомещениях органов криптографической защиты должны исключить:

- возможность пребывания в них пользователей СКЗИ
- возможность неконтролируемого проникновения или пребывания в них посторонних лиц
- возможность просмотра посторонними лицами ведущихся там работ

< Вопрос № 35 >

Процесс зашифрования или расшифрования называется:

- Шифрование
- Шифровка

< Вопрос № 36 >

Как называется гамма по известному фрагменту которой нельзя определить другие ее фрагменты и восстановить со всеми деталями алгоритм, использованный для ее выработки?

- Криптостойкая гамма
- Обычная гамма
- Фрагментарная гамма

< Вопрос № 37 >

Если аппаратные или аппаратно - программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно

- пользователями СКЗИ
- с соответствующими аппаратными средствами

< Вопрос № 38 >

Основные задачи системы информационной безопасности, которые решает PKI:

- исключить возможность подтверждения совершенных пользователями действий с информацией
- обеспечение конфиденциальности информации
- обеспечение целостности информации
- обеспечение аутентификации пользователей и ресурсов, к которым обращаются пользователи

< Вопрос № 39 >

Как называется принцип построения криптографических алгоритмов, согласно которому в секрете держится только определенный набор их параметров (ключ), а все остальное может быть открытым без снижения стойкости алгоритма ниже допустимой величины?

- Принцип Кирхгофа
- Протокол криптографический

< Вопрос № 40 >

Для каких целей в криптографии используются хэш-функция:

- расчета контрольной суммы пакета
- создания образов некоторых данных для их безопасного хранения
- образования так называемых дайджестов h(m) для сообщений m

< Вопрос № 41 >

Уничтожение криптоключей (исходной ключевой информации) может производиться:

- путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования)
- путем физического уничтожения ключевого носителя, на котором они расположены

< Вопрос № 42 >

PKI это:

- Инфраструктура открытых ключей (PKI - Public Key Infrastructure)
- Инфраструктура закрытых ключей (PKI - Private Key Infrastructure)

< Вопрос № 43 >

Первые сведения о применении шифров в военном деле связаны с именем спартанского полководца Лисандра, использовавшего для передачи сообщений шифр -

- шифр Цезаря
- Сцитала

Темы рефератов

1. Шифр Гая Юлия Цезаря
2. Шифр перестановки «сцитала»
3. Диск Энея
4. Квадрат Полибия
5. Шифр Чейза
6. Тюремный шифр
7. Магические квадраты
8. Шифр Аве Мария
9. Таблица Тритемия
10. Шифр Бэкона
11. Шифровальный диск Альберти
12. Шифры Порта
13. Шифр Кардано и Решелье
14. Шифр Виженера
15. Шифр Фальконера
16. Шифр Кеплера и Галилея
17. Алгоритм Берлекэмпа - Мэсси
18. Метод «одноразовых блокнотов»
19. Алгоритм SEAL
20. Методы получения случайных и псевдослучайных чисел
21. Анализ генераторов псевдослучайных чисел

22. Шифр RC 4
23. Роторные машины
24. Атаки на поточные шифры
25. Атаки на блочные шифры
26. Сравнительный анализ блочных и поточных симметричных алгоритмов шифрования
27. Криптосистема Elgamal
28. ГОСТ 34.10-2001
29. DSS
30. Протокол обмена ключами Диффи - Хеллмана
31. Схема идентификации Feige-Fiat-Shamir
32. RSA
33. Triple DES
34. IDEA
35. ГОСТ 28147-89
36. RC5
37. Blowfish
38. AES (Rijndael)
39. CAST
40. Алгоритм Рабина
41. Криптография в Первой мировой войне
42. Криптография в Великой Отечественной войне 1941-1945
43. Система удостоверяющих центров в РФ

Примерный перечень вопросов к зачету по дисциплине для обучающихся

1. Основные понятия криптографии
2. Простейшие методы шифрования с закрытым ключом
3. Принципы построения блочных шифров с закрытым ключом
4. Алгоритмы шифрования DES и AES
5. Алгоритм криптографического преобразования данных ГОСТ 28147-89
6. Криптографические хеш-функции
7. Поточные шифры и генераторы псевдослучайных чисел
8. Введение в криптографию с открытым ключом
9. Основные положения теории чисел, используемые в криптографии с открытым ключом
10. Криптографические алгоритмы с открытым ключом и их использование
11. Электронная подпись
12. Совершенно секретные системы
13. Шифрование, помехоустойчивое кодирование и сжатие информации
14. Проблема распределения секретных ключей.
15. Протокол Диффи–Хеллмана
16. Протоколы распределения секретных ключей, основанные на использовании симметричных шифров
17. Схема разделения секрета
18. Расчет простых пороговых схем разделения секрета
19. Схемы электронной подписи
20. RSA, ECDSA и ГОСТ
21. Сертификаты инфраструктуры открытых ключей и их структура
22. Функции удостоверяющего центра
23. Протоколы «рукопожатия» и идентификации типа «запрос-ответ».
24. Протоколы доказательства знания с нулевым разглашением .
25. Схемы слепой подписи и скрытого канала
26. Протоколы электронного голосования
27. Примеры прикладных протоколов.
28. Шифр перестановки
29. Криптографические средства с древнего времени

30. Основные понятия криптографии
31. Функции, используемые в криптографических системах
32. Однонаправленные функции
33. Имитостойкость
34. Криптографическая стойкость
35. Практическая криптографическая стойкость
36. Классификация поточных шифров
37. Регистр сдвига с линейной обратной связью
38. Линейная сложность
39. Нелинейные регистры сдвига с обратной связью
40. Нелинейная комбинация генераторов
41. Линейное и предварительное шифрование
42. Гаммирование
43. Классификация блочных шифров
44. Режимы использования блочных шифров
45. Режим простой замены
46. Режим шифрования с зацеплением
47. Режим обратной связи по шифротексту
48. Режим шифрования с обратной связью по выходу

Тестовые задания для контроля остаточных знаний по дисциплине

< Вопрос № 1 >

Приказами Росстандарта от 07 августа 2012 г. №№ 215-ст, 216-ст утверждены новые национальные стандарты:

- ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»
- ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (взамен ГОСТ Р 34.10-2001)

< Вопрос № 2 >

Не существует Криптосистем -

- Симметричные
- Ассиметричные
- Параллельные

< Вопрос № 3 >

Назовите одну из причин популярности RSA?

- Возможность гарантированно оценить защищенность
- Высокая по сравнению с симметричными системами производительность

< Вопрос № 4 >

Доверие к средствам криптографической защиты предполагает комплексное решение следующих подзадач:

- Анализ комплекса организационно-технических мер защиты, обеспечивающих заданный уровень криптографической защиты
- Оценка ПО не взаимодействующего с криптографическими сервисами
- Оценка криптографических сервисов
- Исследование криптографических алгоритмов и их реализации

< Вопрос № 5 >

Квалифицированный сертификат должен содержать следующую информацию:

- наименования средств электронной подписи и средств аккредитованного удостоверяющего центра, которые использованы для создания ключа электронной подписи, ключа проверки электронной подписи, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с настоящим Федеральным законом
- фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата - для физического лица либо наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата - для юридического лица
- общий номер квалифицированного сертификата, даты начала и окончания его действия
- ключ проверки электронной подписи

< Вопрос № 6 >

Искуство составления шифров и шифропротоколов -

- Криптография
- Криптоанализ

< Вопрос № 7 >

Доверие к средствам криптографической защиты не предполагает комплексное решение следующих подзадач:

- Оценка влияния программно-аппаратного окружения на корректность работы СКЗИ
- Оценка реализации соответствующего уровня контроля присутствия НДВ
- Доказательство корректности и безопасности целевых функций СКЗИ (формирование защищаемых объектов, отсутствие утечек ключевой информации и т.д.)
- Оценка корректности встраивания криптографических сервисов в прикладное ПО на основе согласованных с ФСБ рекомендаций

< Вопрос № 8 >

Факт того, , что нахождение больших простых чисел в вычислительном отношении осуществляется легко, но разложение на множители произведения двух таких чисел практически невыполнимо, лежит в основе:

- DES
- RSA

< Вопрос № 9 >

Одна из первых книг по шифровке написана -

- аббатом Трителлием (1462-1516) из Германии
- аббатом Трителлием (1416-1466) из Италии

< Вопрос № 10 >

Сертификат ключа проверки электронной подписи прекращает свое действие:

- в связи с истечением установленного срока его действия
- в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам
- в связи с выходным днём
- на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа

< Вопрос № 11 >

Американский специалист по криптографии, имеет звание Профессора имени Эндрю и Эрны Витерби по компьютерным наукам на Факультете электротехники и компьютерных наук (EECS) и состоит в штате кафедры CSAIL в Массачусетском технологическом институте, также является членом лаборатории Теория вычислений и лидером группы Криптография и информационная безопасность?

- Рональд Линн Ривест
- Леонард Макс Адлеман
- Ади Шамир

< Вопрос № 12 >

Видами электронных подписей, , являются:

- простая подпись и усиленная подпсиь
- неквалифицированная электронная подпись и квалифицированная электронная подпись
- простая электронная подпись и усиленная электронная подпись
- усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись

< Вопрос № 13 >

Реализация (распространение) СКЗИ и (или) РКД на них осуществляется юридическим лицом или индивидуальным предпринимателем, имеющим право на осуществление данного вида деятельности, связанного с шифровальными (криптографическими) средствами, на основании:

- лицензии ФТЭК России
- свидетельства об аккредитации МИНКОСВЯЗЬ России
- лицензии ФСБ России

< Вопрос № 14 >

Как называют результаты хеш-функции?

- хеш-кодом
- хеш-кодировкой
- хешем
- сверткой сообщения

< Вопрос № 15 >

Шифр аддитивный это

- Шифр, в котором отдельные символы исходного текста или их группы заменяются на другие символы или группы символов, сохраняя при этом свое положение в тексте относительно других заменяемых групп.
- Шифр гаммирования, в котором для наложения гаммы на данные используется бинарная операция аддитивного типа.
- Шифр, в котором процедура зашифрования заключается в перестановках элементов открытого текста или их групп, сами элементы при этом остаются неизменными.

< Вопрос № 16 >

В соответсвии с каким законом уполномоченным органом по обеспечению криптографическими методами безопасности информационно-телекоммуникационных систем, сетей связи специального назначения и иных сетей связи, обеспечивающих передачу шифрованной информации, на территории Российской Федерации и в её учреждениях за границей, является Федеральная служба безопасности России:

- Федеральный закон Российской Федерации от 27.07.06 года № 149 -ФЗ «Об информации, информационных технологиях и о защите информации»
- Федеральный закон от 03.04.1995 № 40-ФЗ «О Федеральной службе безопасности»

< Вопрос № 17 >

Криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований:

- Вычисление логарифма в конечном поле
- Вычисление корней алгебраических уравнений
- Перестановки таблиц кодировки
- Разложение больших чисел на простые множители

< Вопрос № 18 >

Требования Положения ПКЗ-2005 носят рекомендательный характер при разработке, производстве, реализации и эксплуатации:

- информационно-телекоммуникационных систем, реализующих функции криптографической защиты информации, относящейся к информации конфиденциального характера
- средств криптографической защиты информации, доступ к которой ограничивается по решению обладателя, пользователя (потребителя) данной информации, собственника (владельца) информационных ресурсов (информационных систем) или уполномоченных ими лиц, являющихся государственными органами или организациями, выполняющими государственные заказы
- средств электронной цифровой подписи, предназначаемых для использования в электронном документообороте, информация которого не относится к информации конфиденциального характера
- средств криптографической защиты информации открытых и общедоступных осударственных информационных ресурсов Российской Федерации

< Вопрос № 19 >

Информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается

- равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью
- электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия

< Вопрос № 20 >

Один из самых известных американских криптографов, заслуживший мировую известность за концепцию криптографии с открытым ключом:

- Леонард Макс Адлеман
- Клод Шеннон
- А.Конан Дойл
- Уитфилд Диффи

< Вопрос № 21 >

Как назаваются специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления

ключа криптограммы и обратного преобразования?

- Шифровальные методы защиты информации
- Криптографические методы защиты информации
- Кодировочные методы защиты информации

< Вопрос № 22 >

При обращении в аккредитованный удостоверяющий центр заявитель указывает на ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются) и представляет следующие документы, подтверждающие достоверность информации, предоставленной заявителем для включения в квалифицированный сертификат, либо их надлежащим образом заверенные копии:

- водительское удостоверение
- доверенность или иной документ, подтверждающий право заявителя действовать от имени других лиц
- основной документ, удостоверяющий личность, страховое свидетельство государственного пенсионного страхования заявителя - физического лица или учредительные документы, документ, подтверждающий факт внесения записи о юридическом лице в Единый государственный реестр юридических лиц, и свидетельство о постановке на учет в налоговом органе заявителя - юридического лица
- надлежащим образом заверенный перевод на русский язык документов о государственной регистрации юридического лица в соответствии с законодательством иностранного государства (для иностранных юридических лиц)

< Вопрос № 23 >

ПКЗ-2005 необходимо руководствоваться при разработке, производстве, реализации и эксплуатации средств криптографической защиты информации конфиденциального характера в следующих случаях:

- при обрабатывании информации конфиденциального характера, обладателем которой являются государственные органы или организации, выполняющие государственные заказы, в случае принятия ими мер по охране ее конфиденциальности путем использования средств криптографической защиты
- при обрабатывании информации конфиденциального характера в государственных органах и в организациях, выполняющих государственные заказы, обладатель которой принимает меры к охране ее конфиденциальности путем отмены необходимости криптографической защиты данной информации

< Вопрос № 24 >

Один из самых известных американских криптографов, который получил известность благодаря разработке первой асимметричной криптосистемы в соавторстве с Уитфилдом Диффи и Ральфом Мерклем (1952г)?

- Рональд Линн Ривест
- Леонард Макс Адлеман
- Уитфилд Диффи
- Ади Шамир

< Вопрос № 25 >

Удостоверяющий центр вправе выдавать сертификаты ключей проверки электронных подписей

- в форме документов галограмм
- в форме документов на бумажном носителе
- в форме электронных документов

< Вопрос № 26 >

Как называется система включающая два преобразования – одно для отправителя и одно для получателя, – оба из которых выполняются при использовании того же самого секретного ключа?

- Асимметричная криптографическая система
- Симметричная криптографическая система

< Вопрос № 27 >

При использовании каких алгоритмов требуются более надежные (высоконадежные) механизмы для распределения ключей?

- Алгоритмы с симметричными ключами, так как для шифрования и расшифрования используется один и тот же ключ
- Алгоритмы с асимметричными ключами

< Вопрос № 28 >

ПКЗ-2005 необходимо руководствоваться при разработке, производстве, реализации и эксплуатации средств криптографической защиты информации конфиденциального характера в следующих случаях:

- при организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации
- при организации криптографической защиты информации конфиденциального характера в организациях независимо от их организационно-правовой формы и формы собственности при выполнении ими заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд
- если обязательность защиты информации конфиденциального характера возлагается законодательством Российской Федерации на лиц, имеющих доступ к этой информации или наделенных полномочиями по распоряжению сведениями, содержащимися в данной информации
- если информация конфиденциального характера не подлежит защите в соответствии с законодательством Российской Федерации

< Вопрос № 29 >

Аккредитованный удостоверяющий центр обязан хранить в течение срока его деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федераци, следующую информацию:

- реквизиты всех документов, удостоверяющего личность владельца квалифицированного сертификата - физического лица
- реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица
- сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата
- сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат

< Вопрос № 30 >

Квалифицированной электронной подписью является электронная подпись, которая соответ-

ствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом
- ключ проверки электронной подписи указан в квалифицированном сертификате
- ключа проверки электронной подписи может не создаваться

< Вопрос № 31 >

Как называется криптографический метод заключающийся в том, что символы шифруемого текста переставляются по некоторому правилу в пределах заданного блока передаваемого текста?

- перестановка
- подстановка

< Вопрос № 32 >

В случае принятия решения о прекращении своей деятельности аккредитованный удостоверяющий центр обязан:

- сообщить об этом в уполномоченный федеральный орган не позднее чем за три месяца до даты прекращения своей деятельности
- передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре
- передать в уполномоченный федеральный орган в установленном порядке реестр квалифицированных сертификатов
- сообщить об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности

< Вопрос № 33 >

Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)

- регулирует отношения, возникающие при разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, содержащих сведения, составляющие государственную тайну
- регулирует отношения, возникающие при разработке, производстве, реализации и эксплуатации технических средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну
- регулирует отношения, возникающие при разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

< Вопрос № 34 >

К числу основных недостатков криптографических методов можно отнести следующие:

- высокие требования к сохранности секретных ключей и защиты открытых ключей от подмены
- большие затраты ресурсов (времени, производительности процессоров) на выполнение криптографических преобразований информации
- необходимость защиты открытой информации и ключей от НСД
- высокая гарантированная стойкость защиты

< Вопрос № 35 >

Известный способ шифрования, обладающий сменными элементами - ключами, называтся -

- Криптограммой
- Криптосистемой

< Вопрос № 36 >

Удостоверяющий центр:

- проверяет уникальность ключей проверки электронных подписей в регистре сертификатов
- устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет"
- создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей
- ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных п

< Вопрос № 37 >

Код обнаружения манипуляций

- Код фиксированной длины, вырабатываемый из данных с использованием вычислительно необратимой функции с целью обнаружения факта изменений хранимых или передаваемых по каналу связи данных.
- Имитовставка, код фиксированной длины, вырабатываемый из данных с использованием секретного ключа и добавляемый к данным с целью обнаружения факта изменений хранимых или передаваемых по каналу связи данных.

< Вопрос № 38 >

Код аутентификации это:

- Имитовставка, код фиксированной длины, вырабатываемый из данных с использованием секретного ключа и добавляемый к данным с целью обнаружения факта изменений хранимых или передаваемых по каналу связи данных.
- Код фиксированной длины, вырабатываемый из данных с использованием вычислительно необратимой функции с целью обнаружения факта изменений хранимых или передаваемых по каналу связи данных.

< Вопрос № 39 >

Если в использовании СКЗИ выявлены серьезные нарушения, из-за чего становится реальной утечка конфиденциальной информации, безопасность которой обеспечивается с использованием СКЗИ, то лицензиаты ФСБ России

- вправе дать указание о прекращении использования СКЗИ навсегда
- вправе дать указание о немедленном прекращении использования СКЗИ до устранения причин выявленных нарушений

< Вопрос № 40 >

В состав науки Криптологии не входит-

- Криптоанализ
- Стеганография

- Криптография

< Вопрос № 41 >

Передача по техническим средствам связи криптоключей -

- не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами
- допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами

< Вопрос № 42 >

Известный израильский криптоаналитик, учёный в области теории вычислительных систем, профессор информатики и прикладной математики в институте Вейцмана, лауреат премии Тьюринга:

- Ади Шамир
- Леонард Макс Адлема
- Рональд Линн Ривест

< Вопрос № 43 >

Размещение, специальное оборудование, охрана и организация режима в спецпомещениях органов криптографической защиты должны исключить:

- возможность пребывания в них пользователей СКЗИ
- возможность просмотра посторонними лицами ведущихся там работ
- возможность неконтролируемого проникновения или пребывания в них посторонних лиц

< Вопрос № 44 >

Если аппаратные или аппаратно - программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно

- пользователями СКЗИ
- с соответствующими аппаратными средствами

< Вопрос № 45 >

Как называется гамма по известному фрагменту которой нельзя определить другие ее фрагменты и восстановить со всеми деталями алгоритм, использованный для ее выработки?

- Криптостойкая гамма
- Обычная гамма
- Фрагментарная гамма

< Вопрос № 46 >

Наука (и практика ее применения) о методах и способах вскрытия шифров -

- Криптография
- Криптоанализ

< Вопрос № 47 >

Уничтожение криптоключей (исходной ключевой информации) может производиться:

- путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования)

- путем физического уничтожения ключевого носителя, на котором они расположены

< Вопрос № 48 >

Как называется архитектура построения блочных шифров, доминирующая в настоящее время в традиционной криптографии, в которой весь процесс шифрования блока выполняется за серию шагов (раундов), на каждом из которых блок делится на изменяемую и постоянную части, с помощью функции шифрования из постоянной части и раундового ключа вырабатывается модифицирующий код, который используется для модификации?

- Традиционная архитектура
- Сеть Файстеля

< Вопрос № 49 >

Открытый Ключ это

- Несекретный набор параметров асимметричной криптографической системы, необходимый и достаточный для выполнения отдельных криптографических преобразований.
- Массив незашифрованных данных.

< Вопрос № 50 >

Если криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в

- техническом (аппаратном) журнале, ведущемся непосредственно пользователем СКЗИ
- журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним

7.1. Методические материалы, определяющие процедуры оценивания знаний, умений и навыков, и опыта деятельности, характеризующих этапы формирования компетенций

Требования к написанию реферата

Продукт самостоятельной работы обучающегося, представляющий собой краткое изложение в письменном виде полученных результатов (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.

Реферат должен быть структурирован (по главам, разделам, параграфам) и включать разделы: введение, основная часть, заключение, список использованных источников. В зависимости от тематики реферата к нему могут быть оформлены приложения, содержащие документы, иллюстрации, таблицы, схемы и т.д. Объем реферата – 15-20 страниц печатного текста, включая титульный лист, введение, заключение и список литературы.

Его задачами являются:

1. Формирование умений самостоятельной работы с источниками литературы, их систематизация;
2. Развитие навыков логического мышления;
3. Углубление теоретических знаний по проблеме исследования.

При оценке реферата используются следующие критерии:

- новизна текста;
- обоснованность выбора источника;
- степень раскрытия сущности вопроса;
- соблюдения требований к оформлению.

Критерии оценивания реферата:	
«отлично»	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.
«хорошо»	Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; невыдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.
«удовлетворительно»	Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.
«неудовлетворительно»	Тема реферата не раскрыта, обнаруживается существенное не понимание проблемы.

Тематика рефератов выдается преподавателем в конце семинарского занятия.

Требования к выполнению тестового задания

Тестирование является одним из основных средств формального контроля качества обучения. Это метод, основанный на стандартизированных заданиях, которые позволяют измерить психофизиологические и личностные характеристики, а также знания, умения и навыки испытуемого.

Основные принципы тестирования, следующие:

− связь с целями обучения - цели тестирования должны отвечать критериям социальной полезности и значимости, научной корректности и общественной поддержки;

− объективность - использование в педагогических измерениях этого принципа призвано не допустить субъективизма и предвзятости в процессе этих измерений;

− справедливость и гласность - одинаково доброжелательное отношение ко всем обучающимся, открытость всех этапов процесса измерений, своевременность ознакомления обучающихся с результатами измерений;

− систематичность – систематичность тестирований и самопроверок каждого учебного модуля, раздела и каждой темы; важным аспектом данного принципа является требование репрезентативного представления содержания учебного курса в содержании теста;

- гуманность и этичность - тестовые задания и процедура тестирования должны исключать нанесение какого-либо вреда обучающимся, не допускать ущемления их по национальному, этническому, материальному, расовому, территориальному, культурному и другим признакам;

Важнейшим является принцип, в соответствии с которым тесты должны быть построены по методике, обеспечивающей выполнение требований соответствующего федерального государственного образовательного стандарта.

В тестовых заданиях используются четыре типа вопросов:

− закрытая форма - является наиболее распространенной и предлагает несколько альтернативных ответов на поставленный вопрос. Например, обучающемуся задается вопрос, требующий альтернативного ответа «да» или «нет», «является» или «не является», «относится» или «не относится» и т.п. Тестовое задание, содержащее вопрос в закрытой форме, включает в себя один или несколько правильных ответов и иногда называется выборочным заданием. Закрытая форма вопросов используется также в тестах-задачах с выборочными ответами. В тестовом задании в этом случае сформулированы условие задачи и все необходимые исходные данные, а в

ответах представлены несколько вариантов результата решения в числовом или буквенном виде. Обучающийся должен решить задачу и показать, какой из представленных ответов он получил.

− открытая форма - вопрос в открытой форме представляет собой утверждение, которое необходимо дополнить. Данная форма может быть представлена в тестовом задании, например, в виде словесного текста, формулы (уравнения), графика, в которых пропущены существенные составляющие - части слова или буквы, условные обозначения, линии или изображения элементов схемы и графика. Обучающийся должен по памяти вставить соответствующие элементы в указанные места («пропуски»).

− установление соответствия - в данном случае обучающемуся предлагают два списка, между элементами которых следует установить соответствие;

− установление последовательности - предполагает необходимость установить правильную последовательность предлагаемого списка слов или фраз.

Критерии оценки знаний при проведении тестирования

Отметка «отлично» выставляется при условии правильного ответа не менее чем 85% тестовых заданий;

Отметка «хорошо» выставляется при условии правильного ответа не менее чем 70 % тестовых заданий;

Отметка «удовлетворительно» выставляется при условии правильного ответа не менее 50 %;

Отметка «неудовлетворительно» выставляется при условии правильного ответа менее чем на 50 % тестовых заданий.

Результаты текущего контроля используются при проведении промежуточной аттестации.

Критерии оценки знаний на зачете

Отметка «отлично» - студент глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает теорию с практикой. Магистрант не затрудняется с ответом при видоизменении задания, свободно справляется с задачами, заданиями и другими видами применения знаний, показывает знания законодательного и нормативно-технического материалов, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических работ, обнаруживает умение самостоятельно обобщать и излагать материал, не допуская ошибок.

Отметка «хорошо» - студент твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения и владеет необходимыми навыками при выполнении практических заданий.

Отметка «удовлетворительно» - студент усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий.

Отметка «неудовлетворительно» - студент не знает значительной части программного материала, допускает существенные ошибки, с большими затруднениями выполняет практические работы.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Основная литература

1. Бабаш, А.В. Криптографические методы защиты информации. Т. 3 [Электронный ресурс]: учебно-методическое пособие / А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2014. - 216 с. -

ЭБС «Znanium. com» - Режим доступа: http://znanium.com/catalog.php?bookinfo=432654.

2. Басалова, Г.В. Основы криптографии [Электронный ресурс]/ Басалова Г.В. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 282 с. - ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/52158

3. Калмыков, И.А. Криптографические методы защиты информации [Электронный ресурс]: лабораторный практикум/ И.А. Калмыков, Д.О. Науменко, Т.А. Гиш. - Ставрополь: Северо-Кавказский федеральный университет, 2015. - 109 с. - ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/63099.html .

4. Лапонина, О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс]: учебное пособие/ О.Р. Лапонина. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 242 с. - ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/52217.html.

5. Ларин, Д.А. . Криптографическая деятельность в России от Полтавы до Бородина [Электронный ресурс]: монография/ Д.А, Ларин. - Москва: РИОР: ИНФРА-М, 2015. - 282 с. - ЭБС «Znanium. com» - Режим доступа: http://znanium.com/catalog.php?bookinfo=479196.html.

8.2. Дополнительная литература

1. Ожиганов, А.А. Криптографические системы с секретным и открытым ключом [Электронный ресурс]: учебное пособие/ А.А. Ожиганов. - СПб.: Университет ИТМО, 2015. - 66 с. - ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/67230.html

2. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс]/ А.А. Петров. - Саратов: Профобразование, 2017. - 446 с. - ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/63800.html

3. Практикум по выполнению лабораторных работ по дисциплине Криптографические методы защиты информации [Электронный ресурс]/ [сост. Смирнов А.Э., Пономарёва Ю.А.]. - М.: Московский технический университет связи и информатики, 2015. - 67 с. - ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/61738.html .

8.3. Информационно-телекоммуникационные ресурсы сети «Интернет»

1. Образовательный портал ФГБОУ ВО «МГТУ» [Электронный ресурс]: Режим доступа: https://mkgtu.ru/

2. Официальный сайт Правительства Российской Федерации. [Электронный ресурс]: Режим доступа: http://www.government.ru

3. Информационно-правовой портал «Гарант» [Электронный ресурс]: Режим доступа: http://www.garant.ru/

4. Научная электронная библиотека www.eLIBRARY.RU – Режим доступа: http://elibrary.ru/

5. Электронный каталог библиотеки – Режим доступа: // http://lib.mkgtu.ru:8004/catalog/fol2;

6. Единое окно доступа к образовательным ресурсам: Режим доступа: http://window.edu.ru/

7. Официальный Интернет – ресурс Минкомсвязи России. Свидетельство о регистрации СМИ Эл No ФС77-32622 от 22 июля 2008 г. URL: http://minsvyaz.ru

8. Портал уполномоченного федерального органа в области использования электронной подписи . URL: http://e-trust.gosuslugi.ru

9. Сайт ФСБ России. URL: http://www.fsb.ru/

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Б1.Б.19 Криптографические методы защиты информации

Раздел / Тема с указанием основных учебных элементов	Методы обучения	Способы (формы) обучения	Средства обучения	Формируемые компетенции
1/1 Введение. Основные понятия и определения.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Учебники, учебные пособия, первоисточники	способностью эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях (ПК-15)
2/2 Математические основы криптографии	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия	способностью эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях (ПК-15)
3/3 Историческая криптография	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Учебники, учебные пособия, первоисточники	способностью эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях (ПК-15)
4/4 Современные симметричные шифры	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельно-**	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия, раздаточный материал	способностью эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также вос-

	сти: объяснительно-иллюстративный, репродуктивный			станавливать их работоспособность при внештатных ситуациях (ПК-15)
5/5 Криптография с открытым ключом	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия, , раздаточный материал	способностью эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях (ПК-15)
6/6 Хеширование. Коды аутентичности сообщений. Электронная подпись.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Учебники, учебные пособия	способностью эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях (ПК-15)
7/7 Управление ключами. Распределение симметричных ключей	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Учебники, учебные пособия	способностью эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях (ПК-15)
8/8 Разработка, производство, реализация и эксплуатация шифровальных (криптографических) средств защиты информации	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Учебники, учебные пособия, , раздаточный материал	способностью эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях (ПК-15)

Учебно-методические материалы по практическим (лабораторным) занятиям дисциплины
Б1.Б.19 Криптографические методы защиты информации

№ раздела дисциплины	Наименование практических работ	Методы обучения	Способы (формы) обучения	Средства обучения
1		2	3	4
1. Введение. Основные понятия и определения.	Шифрованная файловая система Windows и Linux.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Устная речь, учебники, учебные пособия, первоисточники
2. Математические основы криптографии	Шифрование диска BitLocker в операционных системах Windows. Средство криптографической защиты информации SecretDisck.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Устная речь, учебники, учебные пособия, раздаточный материал
3. Историческая криптография	Основы криптоанализа симметричных шифров.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Устная речь, учебники, учебные пособия, раздаточный материал
4. Современные симметричные шифры	Аппаратно-программные комплексы шифрования (АПКШ Континент и др.).	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Устная речь, учебники, учебные пособия
5. Криптография с открытым ключом	OpenSSL и LibreSSL. SSL-bump.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Устная речь, учебники, учебные пособия

6. Хеширование Коды аутентичности сообщений. Электронная подпись.	Криптопровайдеры (СКЗИ Крипто-Про CSP и др.).	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Устная речь, учебники, учебные пособия, раздаточный материал
7. Управление ключами. Распределение симметричных ключей.	Удостоверяющие центры (КриптоПро УЦ 2.0 и др.).	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Устная речь, учебники, учебные пособия
8. Разработка, производство, реализация и эксплуатация шифровальных (криптографических) средств защиты информации	Подготовка пакета документов для лицензирования деятельности в области криптографической защиты информации и аккредитации удостоверяющего центра.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Устная речь, учебники, учебные пособия

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, позволяют:

- организовать процесс образования путем визуализации изучаемой информации посредством использования презентаций, учебных фильмов;
- контролировать результаты обучения на основе компьютерного тестирования;
- автоматизировать расчеты аналитических показателей, предусмотренные программой научно-исследовательской работы;
- автоматизировать поиск информации посредством использования справочных систем.

Для осуществления учебного процесса используется свободно распространяемое (бесплатное не требующее лицензирования) программное обеспечение и лицензионное программное обеспечение компаний Microsoft и Kaspersky:

1. Операционная система на базе Linux;
2. Офисный пакет Open Office;
3. Тестовая система собственной разработки, правообладатель ФГБОУ ВО «МГТУ», свидетельство №2013617338.
4. Программные продукты компании Microsoft для государственных образовательных учреждений (Microsoft Open Value Subscription Education Solutions Agreement № V8209819. Срок действия до 07.2018 г.). Пакет включает в себя весь спектр программ (операционные системы разного класса, СУБД, средства разработки, офисный пакет).
5. Антивирусные программы: Endpoint Security - № лицензии 17E0-160128131746407 72.
6. СКЗИ Крипто-Про CSP.

11. Описание материально-технической базы необходимой для осуществления образовательного процесса по дисциплине (модулю)

Наименования специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Специальные помещения		
Учебные аудитории, оснащенные мультимедийным оборудованием 3-1 Лаборатория программирования и защиты информационных процессов в компьютерных системах 3-2	мультимедийный проектор; компьютеры, оргтехника, аудио-, видеотека, справочная литература; таблицы и слайды по специальности; видеофильмы, учебно-методические пособия, плакаты, видеокейсы	Соглашение (подписка) на программные продукты компании Microsoft для государственных образовательных учреждений (Microsoft Open Value Subscription Education Solutions Agreement № V8209819. Срок действия до 07.2018 г.). Пакет включает в себя весь спектр программ (операционные системы разного класса, СУБД, средства разработки, офисный пакет). Антивирусные программы: Kaspersky Endpoint Security - № лицензии 17E0160128-13174640772. Количество: 400

		рабочих мест. Срок действия 1 год.
Помещения для самостоятельной работы		
Читальный зал ФГБОУ ВО «МГТУ»: ул. Первомайская, 191, 3 этаж.	Читальный зал имеет 150 посадочных мест, компьютерное оснащение с выходом в Интернет на 30 посадочных мест; оснащен специализированной мебелью (столы, стулья, шкафы, шкафы выставочные), стационарное мультимедийное оборудование, оргтехника (принтеры, сканеры, ксероксы)	Свободно распространяемое (бесплатное не требующее лицензирования) программное обеспечение: 1. Операционная система на базе Linux; 2. Офисный пакет Open Office; 3. Графический пакет Gimp; 4. Векторный редактор Inkscape; Антивирусные программы: Kaspersky Endpoint Security - № лицензии 17E0160128-13174640772. Количество: 400 рабочих мест. Срок действия 1 год.

Дополнения и изменения в рабочей программе
за 2020/2021учебный год

В рабочую программу для направления (специальности) 10.05.04 Информационно-аналитические системы безопасности вносятся следующие дополнения и изменения:

П. 3. читать в редакции: «Перечень планируемых результатов обучения и воспитания по дисциплине « наименование дисциплины», соотнесенных с планируемыми результатами освоения образовательной программы».

В п. 5.1. Структура дисциплины для очной формы обучения добавить «Виды учебной и воспитательной работы, включая самостоятельную работу и трудоемкость (в часах)

Наименование п. п. 5.5. читать в редакции: «Структура и содержание учебной и воспитательной деятельности при реализации дисциплины»

Добавить п. 5.8. Календарный график воспитательной работы по дисциплине

Модуль 2. Волонтерская (добровольческая) деятельность обучающихся

Дата, место проведения	Название мероприятия	Форма проведения мероприятия	Ответственный	Достижения обучающихся
Ноябрь 2021 МГТУ.	Волонтерская акция по оказанию бесплатной помощи населению в освоении основ кибербезопасности	Индивидуальная	Брикова И. В.	Сформированность ПК-8; ПК-9

Модуль 6. Досуговая, творческая и социально-культурная деятельность по организации и проведению значимых событий и мероприятий

Дата, место проведения	Название мероприятия	Форма проведения мероприятия	Ответственный	Достижения обучающихся
Октябрь 2021 МГТУ	Единый урок «Мы против террора»	Групповая	Чундышко В.Ю.	Сформированность ОПК-1; ПК-8; ПК-9; ПК-10; ПК-11

Дополнения и изменения внесли:
Чундышко В.Ю. _____, Брикова И.В._____,
(должность, Ф.И.О., подпись)

Рабочая программа пересмотрена и одобрена на заседании кафедры информационной безопасности и прикладной информатики

(наименование кафедры)

«25» августа 2021 год

Заведующий кафедрой В. Ю. Чундышко