Приложение

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ЗАЩИТА ИНФОРМАЦИИ

9 Семестр

Раздел 1 Защита информации от умышленных деструктивных воздействий

1.1 Контроль по итогам (КИ) - 8 Неделя

Контроль по итогам изучения раздела дисциплины

Раздел 1 «Защита информации от умышленных деструктивных воздействий»

Контроль по итогам изучения 1 раздела дисциплины подводится на 8 неделе.

Оценка выставляется без проведения дополнительного контроля по совокупности баллов за выполнение контрольной работы.

Вид контроля	Наименование видов контроля	Максимальная положительная оценка в баллах	Минимальная положительная оценка в баллах
КР	Контрольная работа (письменно)	25	15
КИ-8	**Контроль по итогам изучения раздела (**без проведения дополнительного контроля)	**25**	**15**

Комплект заданий для контрольной работы по дисциплине

Тема «Симметричные криптосистемы»

1. Укажите криптоалгоритмы, в которых используется один фиксированный *S*-блок:

А. DES.
Б. RIJNDAEL.
В. RC4.
Г. ГОСТ 28147-89.

2. Укажите криптоалгоритмы, в которых в качестве ключевой информации используется таблица замен *S*-блока, изменяющаяся в процессе шифрования:

А. DES.
Б. RIJNDAEL.
В. RC4.
Г. ГОСТ 28147-89.

3. Укажите разрядность ключевой информации в криптоалгоритме ГОСТ 28147-89:

А. 256 бит.
Б. 768 бит.

В. 56 бит.
Г. Другое.

4. В совершенно секретных криптосистемах после анализа шифротекста противником:

А. Апостериорные вероятности некоторых открытых текстов возрастают относительно их априорных вероятностей.
Б. Апостериорные вероятности всех возможных открытых текстов не меняются относительно их априорных вероятностей.
В. Апостериорные вероятности некоторых открытых текстов снижаются до нуля.
Г. Правильного ответа нет.

5. Укажите криптоалгоритмы, архитектура которых называется сетью Фейстеля:

А. DES.
Б. ГОСТ 28147-89.
В. AES.
Г. MARS.

6. Какие из перечисленных схем шифрования являются схемами гаммирования?

А. AES в режиме OFB.
Б. RC4.
В. A5.
Г. ГОСТ 28147-89 в режиме простой замены.

7. Укажите ложные утверждения:

А. Схема абсолютно стойкого шифра суть схема гаммирования с обратной связью.
Б. При использовании абсолютно стойкого шифра у противника, не знающего ключа, всегда есть возможность вносить предсказуемые изменения в зашифрованный текст.
В. При использовании для шифрования схемы гаммирования наложение псевдослучайной последовательности на последовательность открытых данных может осуществляться только с использованием функции XOR.
Г. Утверждение Б является истинным.

8. На основе какого блочного шифра разработан стандарт криптографической защиты AES?

А. RC6.
Б. MARS.
В. SERPENT.
Г. TWOFISH.
Д. Другое.

9. Укажите ложные утверждения:

А. При синхронном поточном шифровании результат шифрования каждого элемента открытого текста зависит от позиции этого элемента во входном потоке данных.

Б. При синхронном поточном шифровании результат шифрования каждого элемента открытого текста зависит от всех предшествующих элементов во входном потоке данных.
В. Синхронное поточное шифрование суть наложение псевдослучайной последовательности на входную информационную последовательность.
Г. При синхронном поточном шифровании у противника, не знающего ключа, всегда есть возможность вносить предсказуемые изменения в зашифрованный текст.

10. Укажите ложные утверждения:

А. При самосинхронизирующемся поточном шифровании результат шифрования каждого элемента открытого текста зависит от позиции этого элемента во входном потоке данных.
Б. При самосинхронизирующемся поточном шифровании результат шифрования каждого элемента открытого текста зависит от всех предшествующих элементов во входном потоке данных.
В. Самосинхронизирующееся поточное шифрование суть наложение псевдослучайной последовательности на входную информационную последовательность.
Г. При самосинхронизирующемся поточном шифровании у противника, не знающего ключа, всегда есть возможность вносить предсказуемые изменения в зашифрованный текст.

Раздел 2 Разрушающие программные воздействия

2.1 Контроль по итогам (КИ) - 15 Неделя

Контроль по итогам изучения раздела дисциплины

Раздел 2 «Разрушающие программные воздействия»

Контроль по итогам изучения 2 раздела дисциплины подводится на 15 неделе.

Оценка выставляется без проведения дополнительного контроля в соответствии с баллами контрольной работы.

Вид контроля	Наименование видов контроля	Максимальная положительная оценка в баллах	Минимальная положительная оценка в баллах
КР	Контрольная работа (письменно)	25	15
КИ-15	**Контроль по итогам изучения раздела (**без проведения дополнительного контроля)	**25**	**15**

Тема «Асимметричные криптосистемы»

1. Стойкость какой криптосистемы основывается на сложности решения задачи об укладке рюкзака?

А. ECCS.
Б. RSA.
В. AES.
Г. Другое.

2. Укажите криптосистему, на основе которой разработаны государственные стандарты России и США на ЭЦП:

А. AES.
Б. ECCS.
В. RSA.
Г. Криптосистема Эль-Гамаля.

3. Укажите ложные утверждения:

А. В схеме слепой ЭЦП трижды применяется операция шифрования, при этом дважды используется открытый ключ и один раз – закрытый ключ подписывающего.
Б. В схеме слепой ЭЦП трижды используется операция шифрования: для преобразования затемняющего множителя, формирования ЭЦП и проверки ЭЦП.
В. Шифрование затемняющего множителя в схеме слепой ЭЦП необходимо для обеспечения его секретности.
Г. Шифрование затемняющего множителя в схеме слепой ЭЦП необходимо для обеспечения возможности его снятия после формирования ЭЦП.

4. Какие режимы симметричного блочного шифрования могут использоваться при асимметричном шифровании?

А. Counter Mode.
Б. CBC.
В. OFB.
Г. CFB.

5. Укажите ложные утверждения:

А. Режим простой замены не может использоваться при асимметричном шифровании.
Б. Режим гаммирования не может использоваться при асимметричном шифровании.
В. Режим гаммирования с обратной связью не может использоваться при асимметричном шифровании.
Г. Шифрование предназначено только для обеспечения секретности информации.

6. На чем основана стойкость криптосистем с открытым ключом?

А. На секретности ключа зашифрования.
Б. На секретности алгоритма расшифрования.
В. На сложности решения некой математической задачи.
Г. На секретности алгоритма зашифрования.

7. На чем основана стойкость протокола выработки общего секретного ключа?

А. На сложности решения задачи дискретного логарифмирования.
Б. На сложности решения задачи разложения большого целого числа на простые сомножители.
В. На качестве используемых генераторов псевдослучайных чисел.
Г. На сложности решения задачи об укладке рюкзака.

8. Что такое гибридное шифрование?

А. Симметричное шифрование сообщения на сеансовом ключе, который в дальнейшем шифруется с использованием открытого ключа получателя.
Б. Выработка двумя удаленными абонентами общего секретного ключа, который в дальнейшем используется для симметричного шифрования.
В. Последовательное использование симметричного, а затем асимметричного шифрования.
Г. Последовательное использование асимметричного, а затем симметричного шифрования.

9. Для защиты интересов владельца цифровой купюры в централизованной платежной системе используются:

А. Хеширование прекурсора для получения серийного номера цифровой купюры.
Б. Слепая ЭЦП банка-эмитента на серийном номере цифровой купюры.
В. Ведение списка серийных номеров ранее использованных цифровых купюр.
Г. Правильного ответа нет.

10. Для защиты от повторного использования цифровой купюры в централизованной платежной системе применяют:

А. Хеширование прекурсора для получения серийного номера цифровой купюры.
Б. Слепую ЭЦП банка-эмитента на серийном номере цифровой купюры.
В. Ведение списка серийных номеров ранее использованных цифровых купюр.
Г. Правильного ответа нет.

11. Для обеспечения анонимности и неотслеживаемости платежей в централизованной платежной системе используются:

А. Хеширование прекурсора для получения серийного номера цифровой купюры.
Б. Слепая ЭЦП банка-эмитента на серийном номере цифровой купюры.
В. Ведение списка серийных номеров ранее использованных цифровых купюр.
Г. Правильного ответа нет.

12. Для защиты от подделки номинала цифровой купюры в централизованной платежной системе используются:

А. Хеширование прекурсора для получения серийного номера цифровой купюры.
Б. Слепая ЭЦП банка-эмитента на серийном номере цифровой купюры.
В. Ведение списка серийных номеров ранее использованных цифровых купюр.
Г. Правильного ответа нет.

13. В двухключевой криптосистеме для обеспечения секретности информации, пересылаемой от абонента *A* к абоненту *B*, применяют:

А. Открытый ключ *A*.
Б. Открытый ключ *B*.
В. Закрытый ключ *A*.
Г. Закрытый ключ *B*.

14. Для формирования классической ЭЦП на сообщении, пересылаемом от абонента *A* к абоненту *B*, используется:

А. Открытый ключ *A*.
Б. Открытый ключ *B*.
В. Закрытый ключ *A*.
Г. Закрытый ключ *B*.

15. Для проверки классической ЭЦП на сообщении, пересылаемом от абонента *A* к абоненту *B*, используется:

А. Открытый ключ *A*.
Б. Открытый ключ *B*.
В. Закрытый ключ *A*.
Г. Закрытый ключ *B*.

16. Укажите ложные утверждения:

А. Недостаток двухключевых криптосистем – отсутствие юридической значимости пересылаемых электронных документов.
Б. Недостаток двухключевых криптосистем – низкое быстродействие.
В. Недостаток двухключевых криптосистем – возможность подмены открытых ключей.
Г. Для построения двухключевой критптосистемы используется односторонняя функция.

17. Укажите свойства классической ЭЦП:

А. Документ, подписанный ЭЦП, можно копировать сколь угодно много раз.
Б. ЭЦП невозможно подделать.
В. ЭЦП можно хранить и пересылать отдельно от документа.
Г. Правильного ответа нет.

9 Семестр

Зачет

Вопросы к зачёту по дисциплине

1. Функции генераторов псевдослучайных чисел (ГПСЧ) в системах защиты информации (СЗИ)
2. Требования к качественной хеш-функции
3. Требования к качественному шифру
4. Требования к качественному ГПСЧ
5. Модель криптосистемы с секретным ключом
6. Модель криптосистемы с открытым ключом. Криптосистема RSA
7. Протокол выработки общего секретного ключа
8. Протокол электронной цифровой подписи (ЭЦП)
9. Протокол ЭЦП RSA
10. Абсолютно стойкий шифр
11. Протокол слепой ЭЦП RSA
12. Односторонние функции. Односторонние функции с секретом
13. Принципы построения блочных симметричных шифров
14. Классификация шифров
15. Гаммирование. Свойства гаммирования
16. Блочные и поточные шифры
17. ГОСТ 28147-89.
18. Стандарт криптозащиты AES-128
19. Цифровые деньги. Структура и основные транзакции централизованной платежной системы.
20. Методы антивирусной защиты.
21. Разрушающие программные воздействия (РПВ).
22. Недостатки существующих средств защиты от РПВ. Перспективные направления совершенствования методов защиты от РПВ.
23. Ранцевая криптосистема.
24. Процессный подход к построению эффективной СЗИ.
25. Задачи защиты информации (ЗИ) и методы их решения.
26. Причины ненадежности СЗИ.
27. Шифр A5.
28. Шифр RC4.
29. Стохастические методы ЗИ.
30. Протоколы разделения секрета.
31. Протокол аутентификации удаленных абонентов Нидхэма-Шредера.
32. Протокол аутентификации удаленных абонентов Диффи-Хеллмана.
33. Основы теории кодирования. Двоичный симметричный канал. Минимальное кодовое расстояние. Простейший (n, k)-код.
34. Идея стохастического кода. Преобразованный канал связи. Свойства стохастического кода.
35. Контроль хода выполнения программ. Сторожевой процессор.
36. Контролепригодное проектирование. Самотестирование СБИС.
37. Внесение неопределенности в работу средств и объектов защиты.
38. Конструкции криптографических хеш-функций.
39. Классификация ГПСЧ.
40. Криптоалгоритмы, использующие многомерные преобразования.

Методика оценки результатов сдачи зачета

Критерии оценки знаний устанавливаются в соответствии с требованиями к профессиональной подготовке, исходя из действующих учебных планов и программ, с учётом характера будущей практической деятельности выпускника.

«ОТЛИЧНО» (45-50 баллов) - студент владеет знаниями предмета в соответствии с рабочей программой, достаточно глубоко осмысливает дисциплину; самостоятельно, в логической последовательности и исчерпывающе отвечает на вопрос билета, четко формулирует ответ и правильно отвечает на дополнительные вопросы.

«ХОРОШО» (35-44 баллов) - студент владеет знаниями дисциплины почти в полном объеме программы (имеются пробелы знаний только в некоторых, особенно сложных разделах); самостоятельно и отчасти при наводящих вопросах дает полноценный ответ на вопрос билета; не допускает серьезных ошибок при ответах на дополнительные вопросы.

«УДОВЛЕТВОРИТЕЛЬНО» (30-34 баллов) - студент владеет основным объемом знаний по дисциплине; проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками; в процессе ответов допускаются ошибки по существу вопросов.

«НЕУДОВЛЕТВОРИТЕЛЬНО» (ниже 30 баллов) - студент не освоил обязательного минимума знаний предмета; не способен ответить на вопрос билета даже при дополнительных наводящих вопросах экзаменатора.

Итоговая оценка по курсу выставляется в соответствии со следующей таблицей:

Сумма баллов по дисциплине	Зачет	Оценка (ECTS)	Градация
90 - 100	Зачтено	A	Отлично
85 - 89		B	Очень хорошо
75 - 84		C	Хорошо
70 - 74		D	Удовлетворительно
65 - 69			
60 - 64		E	Посредственно
Ниже 60	Не зачтено	F	Неудовлетворительно