Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №1

1. Атаки на криптографические системы и алгоритмы: поясните понятия криптоатака и криптостойкость; информация, доступная злоумышленнику при анализе шифра; основные показатели криптостойкости; приведите и поясните основные методы криптоанализа шифров.

2. Что такое вредоносное ПО, разновидности, цели и задачи его создания и применения?

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Функции межсетевых экранов (Где должен устанавливаться МЭ? Основные задачи, решаемые МЭ. По каким признакам можно классифицировать МЭ? Поясните следующие функции МЭ – фильтрация трафика и выполнение функций посредничества).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №3

1. Поточные шифры: принципы шифрования и расшифрования информации при использовании гаммы (ключевой псевдослучайной последовательности), основные требования к псевдослучайным последовательностям).

2. Какие дефекты ОС могут привести к созданию каналов утечки информации? Приведите и поясните основные уязвимости программного обеспечения.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Шлюз сеансового уровня (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №2

1. Блочные шифры: принципы шифрования и расшифрования информации; режимы функционирования блочных шифров; возможности, которыми обладает злоумышленник при анализе блочного шифра; основные требования к блочному шифру.

2. Поясните метод выявления вредоносных программ на основе сигнатурного поиска, приведите его достоинства и недостатки.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Экранирующий маршрутизатор (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №4

1. Российский стандарт блочного шифрования «Кузнечик»: основные параметры, структура раунда (цикла) шифрования и принцип действия, процедура разворачивания исходного ключа в раундовые (рабочие) подключи, режимы использования.

2. Поясните метод выявления вредоносных программ на основе эвристического поиска, приведите его достоинства и недостатки.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Шлюз прикладного уровня (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №5

1. Асимметричные криптографические системы: причины появления и основные идеи; односторонние функции; факторизация; дискретный логарифм и дискретный корень.

2. Что такое вредоносное ПО, разновидности, цели и задачи его создания и применения?

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Функции межсетевых экранов (Где должен устанавливаться МЭ? Основные задачи, решаемые МЭ. По каким признакам можно классифицировать МЭ? Поясните следующие функции МЭ – фильтрация трафика и выполнение функций посредничества).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №6

1. Криптографический алгоритм RSA: математическая проблема, лежащая в основе алгоритма; принцип формирования открытого и закрытого ключей пользователя; принцип шифрования сообщений; привести пример шифрования сообщения.

2. Какие существуют методы защиты от вредоносного ПО?

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Шлюз сеансового уровня (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №7

1. Хеш-функции: назначение хеш-функций; основные требования к хеш-функциям; привести краткое описание функции хеширования SHA-3.

2. Какие дефекты ОС могут привести к созданию каналов утечки информации? Приведите и поясните основные уязвимости программного обеспечения.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Экранирующий маршрутизатор (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №8

1. Хеш-функции: назначение хеш-функций; основные требования к хеш-функциям; привести краткое описание функции хеширования GOST R 34.11-2012 (Streebog).

2. Поясните метод выявления вредоносных программ на основе сигнатурного поиска, приведите его достоинства и недостатки.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Шлюз прикладного уровня (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №9

1. Протоколы аутентификации с симметричными алгоритмами шифрования (В чем заключается идея строгой аутентификации? Приведите и поясните следующие методы: односторонняя аутентификация, основанная на метках времени; односторонняя аутентификация, основанная на использовании случайных чисел; двусторонняя аутентификация, использующая случайные значения).

2. Что такое вредоносное ПО, разновидности, цели и задачи его создания и применения?

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Функции межсетевых экранов (Где должен устанавливаться МЭ? Основные задачи, решаемые МЭ. По каким признакам можно классифицировать МЭ? Поясните следующие функции МЭ – фильтрация трафика и выполнение функций посредничества).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №10

1. Поточные шифры: принципы шифрования и расшифрования информации при использовании гаммы (ключевой псевдослучайной последовательности), основные требования к псевдослучайным последовательностям).

2. Какие дефекты ОС могут привести к созданию каналов утечки информации? Приведите и поясните основные уязвимости программного обеспечения.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Шлюз сеансового уровня (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №11

1. Атаки на криптографические системы и алгоритмы: поясните понятия криптоатака и криптостойкость; информация, доступная злоумышленнику при анализе шифра; основные показатели криптостойкости; приведите и поясните основные методы криптоанализа шифров.

2. Поясните метод выявления вредоносных программ на основе сигнатурного поиска, приведите его достоинства и недостатки.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Экранирующий маршрутизатор (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №12

1. Блочные шифры: принципы шифрования и расшифрования информации; режимы функционирования блочных шифров; возможности, которыми обладает злоумышленник при анализе блочного шифра; основные требования к блочному шифру.

2. Поясните метод выявления вредоносных программ на основе эвристического поиска, приведите его достоинства и недостатки.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Шлюз прикладного уровня (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №13

1. Российский стандарт блочного шифрования «Кузнечик»: основные параметры, структура раунда (цикла) шифрования и принцип действия, процедура разворачивания исходного ключа в раундовые (рабочие) подключи, режимы использования.

2. Что такое вредоносное ПО, разновидности, цели и задачи его создания и применения?

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Функции межсетевых экранов (Где должен устанавливаться МЭ? Основные задачи, решаемые МЭ. По каким признакам можно классифицировать МЭ? Поясните следующие функции МЭ – фильтрация трафика и выполнение функций посредничества).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №14

1. Криптографический алгоритм RSA: математическая проблема, лежащая в основе алгоритма; принцип формирования открытого и закрытого ключей пользователя; принцип шифрования сообщений; привести пример шифрования сообщения.

2. Какие дефекты ОС могут привести к созданию каналов утечки информации? Приведите и поясните основные уязвимости программного обеспечения.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Шлюз сеансового уровня (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №15

1. Асимметричные криптографические системы: причины появления и основные идеи; односторонние функции; факторизация; дискретный логарифм и дискретный корень.

2. Поясните метод выявления вредоносных программ на основе сигнатурного поиска, приведите его достоинства и недостатки.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Экранирующий маршрутизатор (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №16

1. Хеш-функции: назначение хеш-функций; основные требования к хеш-функциям; привести краткое описание функции хеширования SHA-3.

2. Поясните метод выявления вредоносных программ на основе эвристического поиска, приведите его достоинства и недостатки.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Шлюз прикладного уровня (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №17

1. Хеш-функции: назначение хеш-функций; основные требования к хеш-функциям; привести краткое описание функции хеширования GOST R 34.11-2012 (Streebog).

2. Что такое вредоносное ПО, разновидности, цели и задачи его создания и применения?

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Функции межсетевых экранов (Где должен устанавливаться МЭ? Основные задачи, решаемые МЭ. По каким признакам можно классифицировать МЭ? Поясните следующие функции МЭ – фильтрация трафика и выполнение функций посредничества).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №18

1. Протоколы аутентификации с симметричными алгоритмами шифрования (В чем заключается идея строгой аутентификации? Приведите и поясните следующие методы: односторонняя аутентификация, основанная на метках времени; односторонняя аутентификация, основанная на использовании случайных чисел; двусторонняя аутентификация, использующая случайные значения).

2. Какие дефекты ОС могут привести к созданию каналов утечки информации? Приведите и поясните основные уязвимости программного обеспечения.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Шлюз сеансового уровня (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №19

1. Атаки на криптографические системы и алгоритмы: поясните понятия криптоатака и криптостойкость; информация, доступная злоумышленнику при анализе шифра; основные показатели криптостойкости; приведите и поясните основные методы криптоанализа шифров.

2. Поясните метод выявления вредоносных программ на основе сигнатурного поиска, приведите его достоинства и недостатки.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Экранирующий маршрутизатор (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №20

1. Поточные шифры: принципы шифрования и расшифрования информации при использовании гаммы (ключевой псевдослучайной последовательности), основные требования к псевдослучайным последовательностям).

2. Поясните метод выявления вредоносных программ на основе эвристического поиска, приведите его достоинства и недостатки.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Шлюз прикладного уровня (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №21

1. Блочные шифры: принципы шифрования и расшифрования информации; режимы функционирования блочных шифров; возможности, которыми обладает злоумышленник при анализе блочного шифра; основные требования к блочному шифру.

2. Что такое вредоносное ПО, разновидности, цели и задачи его создания и применения?

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Функции межсетевых экранов (Где должен устанавливаться МЭ? Основные задачи, решаемые МЭ. По каким признакам можно классифицировать МЭ? Поясните следующие функции МЭ – фильтрация трафика и выполнение функций посредничества).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №22

1. Российский стандарт блочного шифрования «Кузнечик»: основные параметры, структура раунда (цикла) шифрования и принцип действия, процедура разворачивания исходного ключа в раундовые (рабочие) подключи, режимы использования.

2. Какие дефекты ОС могут привести к созданию каналов утечки информации? Приведите и поясните основные уязвимости программного обеспечения.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Шлюз сеансового уровня (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №23

1. Асимметричные криптографические системы: причины появления и основные идеи; односторонние функции; факторизация; дискретный логарифм и дискретный корень.

2. Поясните метод выявления вредоносных программ на основе сигнатурного поиска, приведите его достоинства и недостатки.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Экранирующий маршрутизатор (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №24

1. Криптографический алгоритм RSA: математическая проблема, лежащая в основе алгоритма; принцип формирования открытого и закрытого ключей пользователя; принцип шифрования сообщений; привести пример шифрования сообщения.

2. Поясните метод выявления вредоносных программ на основе эвристического поиска, приведите его достоинства и недостатки.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Шлюз прикладного уровня (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №25

1. Хеш-функции: назначение хеш-функций; основные требования к хеш-функциям; привести краткое описание функции хеширования SHA-3.

2. Что такое вредоносное ПО, разновидности, цели и задачи его создания и применения?

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Функции межсетевых экранов (Где должен устанавливаться МЭ? Основные задачи, решаемые МЭ. По каким признакам можно классифицировать МЭ? Поясните следующие функции МЭ – фильтрация трафика и выполнение функций посредничества).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №26

1. Хеш-функции: назначение хеш-функций; основные требования к хеш-функциям; привести краткое описание функции хеширования GOST R 34.11-2012 (Streebog).

2. Какие дефекты ОС могут привести к созданию каналов утечки информации? Приведите и поясните основные уязвимости программного обеспечения.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Шлюз сеансового уровня (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №27

1. Протоколы аутентификации с симметричными алгоритмами шифрования (В чем заключается идея строгой аутентификации? Приведите и поясните следующие методы: односторонняя аутентификация, основанная на метках времени; односторонняя аутентификация, основанная на использовании случайных чисел; двусторонняя аутентификация, использующая случайные значения).

2. Поясните метод выявления вредоносных программ на основе сигнатурного поиска, приведите его достоинства и недостатки.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Экранирующий маршрутизатор (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №28

1. Атаки на криптографические системы и алгоритмы: поясните понятия криптоатака и криптостойкость; информация, доступная злоумышленнику при анализе шифра; основные показатели криптостойкости; приведите и поясните основные методы криптоанализа шифров.

2. Поясните метод выявления вредоносных программ на основе эвристического поиска, приведите его достоинства и недостатки.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Шлюз прикладного уровня (назначение, принцип работы, достоинства и недостатки).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №29

1. Поточные шифры: принципы шифрования и расшифрования информации при использовании гаммы (ключевой псевдослучайной последовательности), основные требования к псевдослучайным последовательностям).

2. Что такое вредоносное ПО, разновидности, цели и задачи его создания и применения?

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Функции межсетевых экранов (Где должен устанавливаться МЭ? Основные задачи, решаемые МЭ. По каким признакам можно классифицировать МЭ? Поясните следующие функции МЭ – фильтрация трафика и выполнение функций посредничества).

Контрольная работа № 2.
Дисциплина «Безопасность информационных технологий»
Билет №30

1. Блочные шифры: принципы шифрования и расшифрования информации; режимы функционирования блочных шифров; возможности, которыми обладает злоумышленник при анализе блочного шифра; основные требования к блочному шифру.

2. Какие дефекты ОС могут привести к созданию каналов утечки информации? Приведите и поясните основные уязвимости программного обеспечения.

3. Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)

4. Шлюз сеансового уровня (назначение, принцип работы, достоинства и недостатки).