**Вопросы к экзамену**

по дисциплине***:***Информационная безопасность и защита информации

1. Основные понятия информационной безопасности. Основные составляющие.
2. Важность и сложность проблемы информационной безопасности.
3. Основные определения и критерии классификации угроз.
4. Наиболее распространенные угрозы доступности.
5. Программные угрозы доступности.
6. Вредоносное программное обеспечение.
7. Основные угрозы целостности. Статическая и динамическая целостность.
8. Основные угрозы конфиденциальности.
9. Что такое компьютерный вирус? Признаки проявления вируса.
10. Классификация компьютерных вирусов – по среде обитания, по степени воздействия, по способам заражения среды обитания, по алгоритмической особенности построения.
11. Европейские критерии безопасности информационных технологий. Адекватность средств защиты. Уровни безопасности системы.
12. Основные руководящие документы Гостехкомиссии и ФСТЭК по вопросам защиты от несанкционированного доступа к информации. Классы защищенности.
13. ГОСТ Р ИСО МЭК 15048-2002 «Общие критерии оценки безопасности информационных технологий». Профиль защиты. функции безопасности. Предложения безопасности.
14. Признаки защищаемой информации. Владельцы защищаемой информации. Понятие «государственная тайна».
15. Основные понятия и определения криптографии.
16. Криптографические механизмы и примитивы. Базовые методы преобразования информации, используемые в криптографии.
17. Криптография с симметричными ключами, общая схема.
18. Симметричные методы шифрования – методы замены.
19. Симметричные методы шифрования – методы многоалфавитной подстагновки.
20. Симметричные методы шифрования – методы гаммирования.
21. Симметричные методы шифрования – методы перестановки.
22. Структура блочного алгоритма симметричного шифрования.

### Требования к блочному алгоритму шифрования

1. Сеть Фейштеля.
2. Алгоритм DES. Преимущества и недостатки криптографии с симметричными ключами.
3. Алгоритм АES. Понятие раунда.
4. ГОСТ 28147-80.
5. Алгоритм криптографического преобразования данных ГОСТ 28147-89.
6. Структура раунда ГОСТ 28147-89.
7. Процедуры шифрования и дешифрования ГОСТ 28147-89.
8. Ассиметричные алгоритмы шифрования. Криптосистема с открытым ключом RSA.
9. ХЕШ-функция. Понятие односторонней функции. Коллизия хэш-функции.
10. Использование блочных алгоритмов шифрования для формирования хэш-функции.
11. «Оранжевая книга» как оценочный стандарт.
12. Понятие композиционного шифра.
13. Поточные шифры. Пример.
14. Генераторы псевдослучайных чисел.
15. Линейный конгруэнтный генератор псевдослучайных чисел
16. Метод Фибоначчи с запаздыванием

### Генератор псевдослучайных чисел на основе алгоритма BBS

1. Ассиметричные алгоритмы шифрования.
2. Схема открытого шифрования.
3. Цифровая подпись на основе алгоритмов с открытым ключом.
4. Схема создания и проверки цифровой подписи.

### Формирование секретных ключей с использованием асимметричных алгоритмов

1. Требования к алгоритмам шифрования с открытым ключом
2. Электронная подпись на основе алгоритма RSA
3. Цифровая подпись на основе алгоритма Эль-Гамаля
4. Стандарт цифровой подписи DSS
5. Стандарт цифровой подписи ГОСТ Р34.10-94
6. Отечественный стандарт ЭЦП: ГОСТ Р34.10-2001.
7. Основные подходы к измерению информации
8. Норма языка и избыточность сообщений
9. Проблемы передачи информации и их комплексное решение
10. Помехоустойчивое кодирование.
11. Принципы сжатии данных.
12. Руководящие документы ФСТЭК России.
13. Административный уровень информационной безопасности.
14. Политика безопасности.
15. Идентификация и аутентификация, управление доступом.

**Критерии оценки:**

* оценка «отлично» выставляется студенту по результатам письменного экзамена, если студент владеет элементарным операционным полем дисциплины, может давать пояснения явлениям и понятиям, прослеживать связь между явлениями, способен анализировать качественно и /или количественно поставленные проблемы. Оценка «отлично» в бально-рейтинговой системе составляет 35-40 балла;
* оценка «хорошо» выставляется студенту по результатам письменного экзамена, если студент владеет элементарным операционным полем дисциплины, может давать пояснения явлениям и понятиям Оценка «отлично» в бально-рейтинговой системе составляет 28-34 балла;
* оценка «удовлетворительно» выставляется студенту по результатам письменного экзамена, если студент владеет элементарным операционным полем дисциплины Оценка «удовлетворительно» в бально-рейтинговой системе составляет 21-27 балла;
* оценка «неудовлетворительно»  выставляется студенту по результатам письменного экзамена, если студент не владеет элементарным операционным полем дисциплины Оценка «неудовлетворительно» в бально-рейтинговой системе составляет менее 21 балла.

Составитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Левченков А.Н.

(подпись)

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2023 г