МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

**УТВЕРЖДАЮ**
Директор НТИ (филиал) СКФУ
Ефанов А.В.
Ф.И.О.
«____» _____ 2022 г.

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине
Информационная безопасность

| | |
|---|---|
| Направление подготовки | 09.03.02 Информационные системы и технологии |
| Направленность (профиль) | Информационные системы и технологии в бизнесе |
| Форма обучения | очная |
| Год начала обучения | 2022 |
| Реализуется в 6 семестре | |

## Введение

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине «Информационная безопасность». Текущий контроль успеваемости и промежуточная аттестация по данной дисциплине – вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля успеваемости и промежуточной аттестации являются получение первичной информацию о ходе и качестве освоения компетенций, а также стимулирование регулярной целенаправленной работы студентов. Для формирования определенного уровня компетенций.

2. ФОС является приложением к программе дисциплины «Информационная безопасность» и в соответствии с образовательной программой высшего образования по направлению подготовки 09.03.02 Информационные системы и технологии.

3. Разработчик: Кочеров Ю. Н., доцент базовой кафедры Регионального индустриального парка, кандидат технических наук

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель:
Мельникова Е.Н. – председатель УМК НТИ (филиал) СКФУ

Члены комиссии:
А.И. Колдаев, и.о. зав. кафедрой информационных систем, электропривода и автоматики
Э.Е. Тихонов, доцент базовой кафедры территории опережающего социально-экономического развития

Представитель организации-работодателя:
Горшков М. Г., директор ООО «Арнест-информационные технологии"

Экспертное заключение: фонд оценочных средств соответствует ОП ВО по направлению подготовки 09.03.02 Информационные системы и технологии и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Информационная безопасность».

05 марта 2022 г.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

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

| Код оцениваемой компетенции, индикатора (ов) | Этап формирования компетенции (№ темы) *(в соответствии с рабочей программой дисциплины)* | Средства и технологии оценки | Вид контроля, аттестация *(текущий/промежуточный)* | Тип контроля *(устный, письменный или с использованием технических средств)* | Наименование оценочного средства |
|---|---|---|---|---|---|
| ИД-1 ОПК-3<br>ИД-2 ОПК-3<br>ИД-3 ОПК-3<br>ИД-1 ОПК-7<br>ИД-2 ОПК-7<br>ИД-3 ОПК-7 | 1-3 | Собеседование | Текущий | Устный | Вопросы для собеседования |
| ИД-1 ОПК-3<br>ИД-2 ОПК-3<br>ИД-3 ОПК-3<br>ИД-1 ОПК-7<br>ИД-2 ОПК-7<br>ИД-3 ОПК-7 | 1-3 | Тестирование | Текущий | Устный | Паспорт фонда тестовых заданий |

## 1. Описание показателей и критериев оценивания на различных этапах их формирования, описание шкал оценивания

| Уровни сформированности компетенци(ий), индикатора (ов) | Дескрипторы | | | |
|---|---|---|---|---|
| | Минимальный уровень не достигнут (Неудовлетворительно) 2 балла | Минимальный уровень (удовлетворительно) 3 балла | Средний уровень (хорошо) 4 балла | Высокий уровень (отлично) 5 баллов |
| ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | | | | |
| Результаты обучения по дисциплине (модулю):<br>*Индикатор:*<br>ИД-1 ОПК-3<br>ИД-2 ОПК-3<br>ИД-3 ОПК-3 | Не удовлетворительно осознает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной | Слабо осознает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; | Осознает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных | Понимает средства защиты информации; угрозы безопасности информации в компьютерных системах; Решает основные этапы |

| | | | | |
|---|---|---|---|---|
| | безопасности;<br>Не удовлетворительно решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности<br>Не удовлетворительно применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; | Слабо решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности<br>Слабо применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; | требований информационной безопасности;<br>Решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности<br>Применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; | построения систем безопасности корпоративных систем;<br>Применяет основные этапы создания комплексной системы защиты информации; |
| ОПК-7 Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем | | | | |
| Результаты обучения по дисциплине (модулю):<br>*Индикатор:*<br>ИД-1 $_{ОПК-7}$<br>ИД-2 $_{ОПК-7}$<br>ИД-3 $_{ОПК-7}$ | Не удовлетворительно понимает предмет и объект защиты информации;<br>краткий обзор современных методов защиты информации;<br>Не удовлетворительно использует методы функциональной безопасности корпоративных систем;<br>Не удовлетворительно применяет методы сообщения и | Слабо понимает предмет и объект защиты информации;<br>краткий обзор современных методов защиты информации;<br>Слабо использует методы функциональной безопасности корпоративных систем;<br>Слабо применяет методы сообщения и шифрования;<br>стеганографии; | Понимает предмет и объект защиты информации;<br>краткий обзор современных методов защиты информации;<br>Использует методы функциональной безопасности корпоративных систем;<br>применяет методы сообщения и шифрования;<br>стеганографии; | Понимает интегрированную систему информационной безопасности;<br>защита документооборота в вычислительных системах;<br>средства защиты информации;<br>применяет моделирования комплексных систем защиты информации;<br>методы оценки |

| | | | | |
|---|---|---|---|---|
| | шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом; | кодирования; алгоритмы шифрования с открытым ключом; | кодирования; алгоритмы шифрования с открытым ключом; | систем защиты информации; применяет навыки создания алгоритмов шифрования с закрытым ключом; криптографические средства защиты; |

**Описание шкалы оценивания**

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации.

**Текущий контроль**

**Рейтинговая оценка знаний студента (в случаях, предусмотренных нормативными актами СКФУ).**

| № п/п | Вид деятельности студентов | Сроки выполнения | Количество баллов |
|---|---|---|---|
| 5 семестр | | | |
| 1 | Собеседование по темам 1-3, Защита практических работ | 8 | 25 |
| 2 | Собеседование по теме 2-3, Защита лабораторных работ | 16 | 30 |
| | Итого за 5 семестр: | | 55 |
| | Итого: | | 55 |

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

| ***Уровень выполнения контрольного задания*** | ***Рейтинговый балл (в % от максимального балла за контрольное задание)*** |
|---|---|
| *Отличный* | ***100*** |
| *Хороший* | ***80*** |
| *Удовлетворительный* | ***60*** |
| *Неудовлетворительный* | ***0*** |

**Промежуточная аттестация**

Промежуточная аттестация в форме **зачета или зачета с оценкой**

Процедура зачета (зачета с оценкой) как отдельное контрольное мероприятие не проводится, оценивание знаний обучающегося происходит по результатам текущего контроля.

Зачет выставляется по результатам работы в семестре, при сдаче всех контрольных точек, предусмотренных текущим контролем успеваемости. Если по итогам семестра

обучающийся имеет от 33 до 60 баллов, ему ставится отметка «зачтено». Обучающемуся, имеющему по итогам семестра менее 33 баллов, ставится отметка «не зачтено».

Количество баллов за зачет ($S_{зач}$) при различных рейтинговых баллах по дисциплине по результатам работы в семестре

| **Рейтинговый балл по дисциплине по результатам работы в семестре ($R_{сем}$)** | **Количество баллов за зачет ($S_{зач}$)** |
|---|---|
| **$50 \le R_{сем} \le 60$** | **40** |
| **$39 \le R_{сем} < 50$** | **35** |
| **$33 \le R_{сем} < 39$** | **27** |
| **$R_{сем} < 33$** | **0** |

При зачете с оценкой используется шкала пересчета рейтингового балла по дисциплине в оценку по 5-балльной системе

*Шкала пересчета рейтингового балла по дисциплине в оценку по 5-балльной системе*

| ***Рейтинговый балл по дисциплине*** | ***Оценка по 5-балльной системе*** |
|---|---|
| ***88 – 100*** | *Отлично* |
| ***72 – 87*** | *Хорошо* |
| ***53 – 71*** | *Удовлетворительно* |
| ***< 53*** | *Неудовлетворительно* |

## 2. Типовые контрольные задания и иные материалы, характеризующие этапы формирования компетенций

**Вопросы для собеседования**

### Пороговый уровень

**Тема 1. Средства защиты информации**

1. Что такое LFSR?
2. Как построить псевдослучайный генератор на основе регистра сдвига?
3. На чем базируется стойкость генераторов псевдослучайных чисел, исследованных в лабораторной работе?
4. Как реализовать возведение в степень чисел большой разрядности по большому модулю?
5. Какая информация является конфиденциальной?
6. Что относится к защищаемой информации?
7. Что понимается под политикой безопасности?
8. Что понимается под несанкционированным воздействием на защищаемую информацию?
9. Дайте понятие конфиденциальности, целостности и доступности информации.

**Тема 2. Функциональная безопасность корпоративных систем**

1. Что такое симметричное шифрование?
2. В чем особенность блочных шифров?
3. В чем особенность асимметричных систем шифрования?
4. На чем базируется криптостойкость RSA?
5. Как увеличить производительность системы шифрования RSA?
6. Составляющие функциональной безопасности

7. Этапы построения систем безопасности

### Тема 3. Криптографические средства защиты

1. Назначение цифровой подписи.
2. В чем отличие криптосхемы ЭльГамаля от RSA?
3. Почему шифр RSA называется асимметричным?
4. На чем основана стойкость шифра RSA?
5. Что такое цифровой конверт?
6. Опишите общую схему ЭЦП.
7. Каково назначение хеш-функции?
8. Какими свойствами противодействия должна обладать криптографическая хеш-функция?
9. Что такое MAC и как он формируется?

## Повышенный уровень

### Тема 1. Средства защиты информации

1. Какие тесты на случайность вам известны?
2. Сравните результаты тестов генераторов из первой лабораторной работы с тестами второй работы
3. Дайте определение информационной безопасности.
4. Какие цели и задачи включает в себя концепция национальной безопасности РФ?
5. Перечислите основные виды угроз информационной безопасности РФ.
6. Дайте определение комплексного обеспечения информационной безопасности.
7. Перечислите основные элементы организационной основы государственной системы обеспечения информационной безопасности РФ

### Тема 2. Функциональная безопасность корпоративных систем

1. Какова длина ключа блочного шифра?
2. На чем базируется криптостойкость блочного шифра?
3. Какие элементарные операции используются в симметричном шифровании?
4. Какие атаки на систему RSA вам известны?
5. Как противодействовать атакам на систему RSA?
6. Анализ рисков и показатели функциональной безопасности

### Тема 3. Криптографические средства защиты

1. На чем базируется криптостойкость системы ЭльГамаля?
2. Почему шифр RSA называется асимметричным?
3. На чем основана стойкость шифра RSA?
4. Что такое цифровой конверт?
5. Опишите общую схему ЭЦП.
6. Каково назначение хеш-функции?
7. Какими свойствами противодействия должна обладать криптографическая хеш-функция?
8. Что такое MAC и как он формируется?
9. Каковы функции удостоверяющего центра ЭП? Какие сведения заносятся в сертификат открытого ключа ЭП?

10. Для каких целей используется СКЗИ «Верба-OW»?
11. Какие отечественные криптоалгоритмы реализуются в «КриптоПро CSP»?
12. Каково назначение ПАК «КриптоПро УЦ»?

**Компетентностно-ориентированные задания**

1. Проанализировать, 4-битовый LFSR с отводом от первого и четвертого битов со значением 1010
2. Для сообщения длинно 4 бита, шифруемого алгоритмом RSA задаются начальные параметры: генерируется два секретных больших простых числа p и q, необходимо вычислить $n$ и $\varphi(n)$
3. Изобразите схему конструкции Фейстеля и поясните ее
4. Изобразите схема DES-преобразования
5. Рассчитайте значение $1570^{1019} \bmod 3337$
6. Для генерации пары ключей для сообщения длинной 4 вычислите открытый и закрытый ключи

**1. Критерии оценивания компетенций***

Оценка «отлично» выставляется студенту, если он

Понимает средства защиты информации; угрозы безопасности информации в компьютерных системах;

Решает основные этапы построения систем безопасности корпоративных систем;

Применяет основные этапы создания комплексной системы защиты информации;

Понимает интегрированную систему информационной безопасности; защита документооборота в вычислительных системах; средства защиты информации;

применяет моделирования комплексных систем защиты информации; методы оценки систем защиты информации;

применяет навыки создания алгоритмов шифрования с закрытым ключом; криптографические средства защиты;

Оценка «хорошо» выставляется студенту, если он

Осознает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Понимает предмет и объект защиты информации; краткий обзор современных методов защиты информации;

Использует методы функциональной безопасности корпоративных систем;

применяет методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;

Оценка «удовлетворительно» выставляется студенту, если он

Слабо осознает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Слабо решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Слабо применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Слабо понимает предмет и объект защиты информации; краткий обзор современных методов защиты информации;

Слабо использует методы функциональной безопасности корпоративных систем;

Слабо применяет методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;

Оценка «неудовлетворительно» выставляется студенту, если он

Не удовлетворительно осознает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Не удовлетворительно решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Не удовлетворительно применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Не удовлетворительно понимает предмет и объект защиты информации; краткий обзор современных методов защиты информации;

Не удовлетворительно использует методы функциональной безопасности корпоративных систем;

Не удовлетворительно применяет методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;

**2. Описание шкалы оценивания**

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

| Уровень выполнения контрольного задания | Рейтинговый балл (в % от максимального балла за контрольное задание) |
|---|---|
| Отличный | **100** |
| Хороший | **80** |
| Удовлетворительный | **60** |
| Неудовлетворительный | **0** |

**3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Пример:

Процедура проведения данного оценочного мероприятия включает в себя: защиту лабораторных и практических занятий

Предлагаемые студенту вопросы позволяют проверить ИД-1 $_{ОПК-3}$, ИД-2 $_{ОПК-3}$, ИД-3 $_{ОПК-3}$, ИД-1 $_{ОПК-7}$, ИД-2 $_{ОПК-7}$, ИД-$_{3\ ОПК-7}$ компетенции

Для подготовки к данному оценочному мероприятию необходимо 10 минут.

При подготовке к ответу студенту предоставляется право пользования отчетами о выполненных лабораторных и практических занятий.

При проверке задания, оцениваются последовательность и логика ответа

**Оценочный лист**

| № п/п | Фамилия, имя студента | Вид работы | | | | | | Итог |
|---|---|---|---|---|---|---|---|---|
| | | Соответствие ответа заданию | Раскрытие проблемы, темы | Ясность, четкость, логичность, научность изложения | Обоснованность излагаемой позиции, ответа | Самостоятельность в формулировке позиции | Четкость, обоснованность, научность выводов | |
| | | | | | | | | |
| | | | | | | | | |

# Паспорт фонда тестовых заданий по дисциплине Информационная безопасность

| № п/п | Тест | Ключ |
|---|---|---|
| **1.** | Какова цель использования генераторов псевдослучайных чисел при поточном шифровании?<br>– формирование открытых ключей<br>– защита информации от всех случайных или преднамеренных изменений<br>– получение «бесконечной» гаммы (ключевой последовательности), располагая относительно малой длиной самого секретного ключа<br>– защита информации от случайных помех при передаче и хранении<br>– сжатие информации | получение «бесконечной» гаммы (ключевой последовательности), располагая относительно малой длиной самого секретного ключа |
| **2.** | Чем определяется разрядность сдвигового регистра с обратной связью?<br>– скоростью работы регистра<br>– температурой окружающей среды<br>– количеством входов в устройстве генерации функции обратной связи<br>– количеством бит, которое может одновременно храниться в регистре сдвига | количеством бит, которое может одновременно храниться в регистре сдвига |
| **3.** | Математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, называется в криптографии<br>– функцией Диффи-Хеллмана<br>– односторонней функцией<br>– функцией Эйлера<br>– криптографической функцией | односторонней функцией |
| **4.** | Алгоритм ГОСТ 28147-89 является<br>– алгоритмом вычисления функции хеширования<br>– блочным алгоритмом асимметричного шифрования | блочным алгоритмом симметричного шифрования |

| | | |
|---|---|---|
| | – блочным алгоритмом симметричного шифрования<br>– алгоритмом формирования электронной цифровой подписи | |
| **5.** | Что является особенностью использования режима CBC блочного шифра?<br>– одинаковые сообщения при использовании разных векторов инициализации преобразуются в одинаковый шифротекст<br>– сообщение, зашифрованное в данном режиме, можно расшифровать, выбирая блоки шифротекста в произвольном порядке<br>– одинаковые блоки исходного текста преобразуются в одинаковый шифротекст<br>– этот режим работает очень медленно, что практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений<br>– сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока | сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока |
| **6.** | Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0B5 и 37? Варианты ответов представлены в двоичной системе счисления<br>Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид | 10000010 |
| **7.** | Может ли шифр с конечным ключом быть совершенным?<br>– да, если это алгоритм шифрования с открытым ключом<br>– в зависимости от параметров шифра<br>– нет<br>– да | нет |
| **8.** | Что общего имеют все методы шифрования с закрытым ключом?<br>– в них для шифрования информации используется один ключ, а для расшифрования – другой ключ<br>– в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов<br>– в них для операций шифрования и расшифрования используется два разных ключа – открытый и закрытый<br>– в них для шифрования и расшифрования информации используется один и тот же ключ | в них для шифрования и расшифрования информации используется один и тот же ключ |
| **9.** | Для чего предназначен алгоритм Блюм-Блюма-Шуба (BBS)?<br>– генерации псевдослучайных чисел | генерации псевдослучайных чисел |

| | | |
|---|---|---|
| | – для сжатия информации<br>– для формирования открытых ключей<br>– для формирования хеш-кода | |
| **10.** | Выберите вариант ответа, содержащий только простые числа<br>– 2, 5, 19, 37, 59, 101<br>– 2, 7, 17, 37, 57, 107<br>– 2, 5, 19, 37, 59, 133<br>– 3, 7, 19, 39, 59, 10 | 2, 5, 19, 37, 59, 101 |
| **11.** | К правовым методам, обеспечивающим информационную безопасность, относятся:<br>– Разработка аппаратных средств обеспечения правовых данных<br>– Разработка и установка во всех компьютерных правовых сетях журналов учета действий<br>– Разработка и конкретизация правовых нормативных актов обеспечения безопасности | Разработка и конкретизация правовых нормативных актов обеспечения безопасности |
| **12.** | Основными источниками угроз информационной безопасности являются все указанное в списке:<br>– Хищение жестких дисков, подключение к сети, инсайдерство<br>– Перехват данных, хищение данных, изменение архитектуры системы<br>– Хищение данных, подкуп системных администраторов, нарушение регламента работы | Перехват данных, хищение данных, изменение архитектуры системы |
| **13.** | **Виды информационной безопасности:**<br>– Персональная, корпоративная, государственная<br>– Клиентская, серверная, сетевая<br>– Локальная, глобальная, смешанная | Персональная, корпоративная, государственная |
| **14.** | Цели информационной безопасности – своевременное обнаружение, предупреждение:<br>– несанкционированного доступа, воздействия в сети<br>– инсайдерства в организации<br>– чрезвычайных ситуаций | |
| **15.** | Основные объекты информационной безопасности:<br>– Компьютерные сети, базы данных<br>– Информационные системы, психологическое состояние пользователей<br>– Бизнес-ориентированные, коммерческие системы | Компьютерные сети, базы данных |
| **16.** | Основными рисками информационной безопасности являются:<br>– Искажение, уменьшение объема, перекодировка информации<br>– Техническое вмешательство, выведение из строя оборудования сети<br>– Потеря, искажение, утечка информации | Потеря, искажение, утечка информации |

| | | |
|---|---|---|
| **17.** | К основным принципам обеспечения информационной безопасности относится:<br>– Экономической эффективности системы безопасности<br>– - Многоплатформенной реализации системы<br>– - Усиления защищенности всех звеньев системы | Экономической эффективности системы безопасности |
| **18.** | Основными субъектами информационной безопасности являются:<br>– руководители, менеджеры, администраторы компаний<br>– органы права, государства, бизнеса<br>– сетевые базы данных, фаерволлы | органы права, государства, бизнеса |
| **19.** | К основным функциям системы безопасности можно отнести все перечисленное:<br>– Установление регламента, аудит системы, выявление рисков<br>– Установка новых офисных приложений, смена хостинг-компании<br>– Внедрение аутентификации, проверки контактных данных пользователей | Установление регламента, аудит системы, выявление рисков |
| **20.** | Принципом информационной безопасности является принцип недопущения:<br>– Неоправданных ограничений при работе в сети (системе)<br>– Рисков безопасности сети, системы<br>– Презумпции секретности | Неоправданных ограничений при работе в сети (системе) |
| **21.** | Принципом политики информационной безопасности является принцип:<br>– Невозможности миновать защитные средства сети (системы)<br>– Усиления основного звена сети, системы<br>– Полного блокирования доступа при риск-ситуациях | Невозможности миновать защитные средства сети (системы) |
| **22.** | Принцип Кирхгофа:<br>– Секретность ключа определена секретностью открытого сообщения<br>– Секретность информации определена скоростью передачи данных<br>– Секретность закрытого сообщения определяется секретностью ключа | Секретность закрытого сообщения определяется секретностью ключа |
| **23.** | ЭЦП – это:<br>– Электронно-цифровой преобразователь<br>– Электронно-цифровая подпись<br>– Электронно-цифровой процессор | Электронно-цифровая подпись |
| **24.** | Наиболее распространены угрозы информационной безопасности корпоративной системы:<br>– Покупка нелицензионного ПО<br>– Ошибки эксплуатации и неумышленного изменения режима работы системы<br>– Сознательного внедрения сетевых вирусов | Ошибки эксплуатации и неумышленного изменения режима работы системы |

| | | |
|---|---|---|
| **25.** | Наиболее распространены средства воздействия на сеть офиса:<br>– Слабый трафик, информационный обман, вирусы в интернет<br>– Вирусы в сети, логические мины (закладки), информационный перехват<br>– Компьютерные сбои, изменение администрирования, топологии | Вирусы в сети, логические мины (закладки), информационный перехват |
| **26.** | Утечкой информации в системе называется ситуация, характеризуемая:<br>– Потерей данных в системе<br>– Изменением формы информации<br>– Изменением содержания информации | Потерей данных в системе |
| **27.** | Угроза информационной системе (компьютерной сети) – это:<br>– Вероятное событие<br>– Детерминированное (всегда определенное) событие<br>– Событие, происходящее периодически | Вероятное событие |
| **28.** | Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:<br>– Регламентированной<br>– Правовой<br>– Защищаемой | |
| **29.** | Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:<br>– Программные, технические, организационные, технологические<br>– Серверные, клиентские, спутниковые, наземные<br>– Личные, корпоративные, социальные, национальные | Программные, технические, организационные, технологические |
| **30.** | Что такое «минимальное кодовое расстояние»?<br>– характеристика помехоустойчивого кода, показывающая, насколько увеличена длина кодового слова по сравнению с обычным непомехоустойчивым кодом<br>– число разрядов двух кодовых слов, в которых они различны<br>– число контрольных разрядов в кодовом слове<br>– наименьшее из всех расстояний по Хэммингу для любых пар различных кодовых слов, образующих код | наименьшее из всех расстояний по Хэммингу для любых пар различных кодовых слов, образующих код |

**1. Критерии оценивания компетенций***

Оценка «отлично» выставляется студенту, если он

Понимает средства защиты информации; угрозы безопасности информации в компьютерных системах;

Решает основные этапы построения систем безопасности корпоративных систем;

Применяет основные этапы создания комплексной системы защиты информации;

Понимает интегрированную систему информационной безопасности; защита документооборота в вычислительных системах; средства защиты информации;

применяет моделирования комплексных систем защиты информации; методы оценки систем защиты информации;

применяет навыки создания алгоритмов шифрования с закрытым ключом; криптографические средства защиты;

Оценка «хорошо» выставляется студенту, если он

Осознает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Понимает предмет и объект защиты информации; краткий обзор современных методов защиты информации;

Использует методы функциональной безопасности корпоративных систем;

применяет методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;

Оценка «удовлетворительно» выставляется студенту, если он

Слабо осознает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Слабо решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Слабо применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Слабо понимает предмет и объект защиты информации; краткий обзор современных методов защиты информации;

Слабо использует методы функциональной безопасности корпоративных систем;

Слабо применяет методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;

Оценка «неудовлетворительно» выставляется студенту, если он

Не удовлетворительно осознает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Не удовлетворительно решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Не удовлетворительно применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Не удовлетворительно понимает предмет и объект защиты информации; краткий обзор современных методов защиты информации;

Не удовлетворительно использует методы функциональной безопасности корпоративных систем;

Не удовлетворительно применяет методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;