

Компонент ОПОП 27.03.05 Инноватика, направленность (профиль) «Управление  
инновационной деятельностью»  
наименование ОПОП

Б1.О.25  
шифр дисциплины

## ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Дисциплины  
(модуля)

Информационная безопасность

---

Разработчик (и):

Л.Б. Сенецкая  
ФИО

доцент  
должность

К.Э.Н., доцент

ученая степень,  
звание

Утверждено на заседании кафедры

информационных технологий  
наименование кафедры

протокол № 6 от 01.02.2024

Заведующий кафедрой ИТ

  
подпись

Ляш О.И.  
ФИО

## 1. Критерии и средства оценивания компетенций и индикаторов их достижения, формируемых дисциплиной (модулем)

Код и наименование компетенции	Код и наименование индикатора(ов) достижения компетенции	Результаты обучения по дисциплине (модулю)			Оценочные средства текущего контроля	Оценочные средства промежуточной аттестации
		<i>Знать</i>	<i>Уметь</i>	<i>Владеть</i>		
ОПК-7. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ИД-1ОПК-7: - знает принципы работы современных информационных технологий; ИД-2ОПК-7: - решает задачи управления инновационной деятельностью с использованием современных информационных технологий; ИД-3 ОПК-7: -умеет управлять инновационной деятельностью с использованием современных информационных технологий	принципы работы современных информационных технологий, в том числе в части обеспечения информационной безопасности	решать задачи управления инновационной деятельностью с использованием современных информационных технологий с учетом безопасности;	основными принципам и обеспеченная информационной безопасностью на предприятии	- комплект заданий для выполнения практических работ; .-учет посещаемости; -тестовые наборы	Результаты текущего контроля

## 2. Оценка уровня сформированности компетенций (индикаторов их достижения)

Показатели оценивания компетенций (индикаторов их достижения)	Шкала и критериооценки уровня сформированности компетенции			
	Ниже порогового («неудовлетворительно»)	Пороговый («удовлетворительно»)	Продвинутый («хорошо»)	Высокий («отлично»)
<b>Полнота знаний</b>	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущены не грубые ошибки.	Уровень знаний в объеме, соответствующем программе подготовки. Допущены некоторые погрешности.	Уровень знаний в объеме, соответствующем программе подготовки.
<b>Наличие умений</b>	При выполнении стандартных заданий не продемонстрированы	Продемонстрированы основные умения. Выполнены	Продемонстрированы все основные умения. Выполнены все	Продемонстрированы все основные умения. Выполнены все

	ы основные умения. Имели место грубые ошибки.	типовые задания с не грубыми ошибками. Выполнены все задания, но не в полном объеме (отсутствуют пояснения, неполные выводы)	основные задания с некоторыми погрешностями. Выполнены все задания в полном объеме, но некоторые с недочетами.	основные и дополнительные задания без ошибок и погрешностей. Задания выполнены в полном объеме без недочетов.
<b>Наличие навыков (владение опытом)</b>	При выполнении стандартных заданий не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для выполнения стандартных заданий с некоторыми недочетами.	Продемонстрированы базовые навыки при выполнении стандартных заданий с некоторыми недочетами.	Продемонстрированы все основные умения. Выполнены все основные и дополнительные задания без ошибок и погрешностей. Продемонстрирован творческий подход к решению нестандартных задач.
<b>Характеристика сформированности компетенции</b>	Компетенции фактически не сформированы. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач.	Сформированность компетенций соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач.	Сформированность компетенций в целом соответствует требованиям. Имеющихся знаний, умений, навыков достаточно для решения стандартных профессиональных задач.	Сформированность компетенций полностью соответствует требованиям. Имеющихся знаний, умений, навыков в полной мере достаточно для решения сложных, в том числе нестандартных, профессиональных задач.

### 3. Критерии и шкала оценивания заданий текущего контроля

#### 3.1 Критерии и шкала оценивания лабораторных/практических работ

Перечень лабораторных/практических работ описание порядка выполнения и защиты работы, требования к результатам работы, структуре и содержанию отчета и т.п. представлены в методических материалах по освоению дисциплины (модуля) и в электронном курсе в ЭИОС МГТУ.

Оценка/баллы	Критерии оценивания
<i>Отлично</i>	Задание выполнено полностью и правильно. Отчет по лабораторной/практической работе подготовлен качественно в соответствии с требованиями. Полнота ответов на вопросы преподавателя при защите работы.
<i>Хорошо</i>	Задание выполнено полностью, но нет достаточного обоснования или при верном решении допущена незначительная ошибка, не влияющая на правильную последовательность рассуждений. Все требования, предъявляемые к работе, выполнены.
<i>Удовлетворительно</i>	Задания выполнены частично с ошибками. Демонстрирует средний уровень выполнения задания на лабораторную/практическую работу. Большинство требований, предъявляемых к заданию, выполнены.
<i>Неудовлетворительно</i>	Задание выполнено со значительным количеством ошибок на низком уровне. Многие требования, предъявляемые к заданию, не выполнены. ИЛИ Задание не выполнено.

#### 3.2 Критерии и шкала оценивания контрольной работы

Перечень контрольных заданий, рекомендации по выполнению представлены в методических материалах по освоению дисциплины (модуля) и в электронном курсе в ЭИОС МГТУ.

Контрольная работа представляет собой формирование электронного конспекта нормативных документов в области обеспечения информационной безопасности.

Перечень документов предназначенных для конспектирования представлен в ЭИОС.

Оценка/баллы	Критерии оценивания
<i>Отлично</i>	Работа выполнена полностью, без ошибок (возможна одна неточность, описка, не являющаяся следствием непонимания материала).
<i>Хорошо</i>	Работа выполнена полностью, но обоснования шагов решения недостаточны, допущена одна негрубая ошибка или два-три недочета, не влияющих на правильную последовательность рассуждений.
<i>Удовлетворительно</i>	В работе допущено более одной грубой ошибки или более двух-трех недочетов, но обучающийся владеет обязательными умениями по проверяемой теме.
<i>Неудовлетворительно</i>	В работе есть грубые ошибки и недочеты ИЛИ Контрольная работа не выполнена.

#### 3.3 Критерии и шкала оценивания расчетно-графической работы

Перечень контрольных заданий, рекомендации по выполнению представлены в методических материалах по освоению дисциплины (модуля) и в электронном курсе в ЭИОС МГТУ.

В ФОС включены варианты задания.

##### Вариант 1

Написать программу на языке программирования реализации кодирования по методу Плейфера

**Вариант 2**

Написать программу на языке программирования реализации кодирования по методу Полибия

**Вариант 3**

Написать программу на языке программирования реализации кодирования по методу Цезаря

**Вариант 4**

Написать программу на языке программирования реализации кодирования по методу телефона

**Вариант 5**

Написать программу на языке программирования реализации кодирования по методу RSA

Оценка/баллы	Критерии оценивания
<i>Отлично</i>	Работа выполнена полностью, без ошибок (возможна одна неточность, описка, не являющаяся следствием непонимания материала).
<i>Хорошо</i>	Работа выполнена полностью, но обоснования шагов решения недостаточны, допущена одна негрубая ошибка или два-три недочета, не влияющих на правильную последовательность рассуждений.
<i>Удовлетворительно</i>	В работе допущено более одной грубой ошибки или более двух-трех недочетов, но обучающийся владеет обязательными умениями по проверяемой теме.
<i>Неудовлетворительно</i>	В работе есть грубые ошибки и недочеты ИЛИ Контрольная работа не выполнена.

3.3 Критерии и шкала оценивания посещаемости занятий

Посещение занятий обучающимися определяется в процентном соотношении

Баллы	Критерии оценки
10	посещаемость 75 - 100 %
5	посещаемость 50 - 74 %
0	посещаемость менее 50 %

3.4 Критерии и шкала оценивания тестирования

Перечень тестовых вопросов и заданий, описание процедуры тестирования представлены в методических материалах по освоению дисциплины (модуля) и в электронном курсе в ЭИОС МАУ.

В ФОС включен типовой вариант тестового задания:

1. Информационное оружие-это...?

комплекс мер направленных на изменение индивидуального и общественного сознания;

\*комплекс методов, средств и технологий предназначенных для распространения дезинформации в системе формирования общественного сознания;

комплекс нормативно-правовой документации;

2 Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена- это...

\*конфиденциальность;

целостность;

доступность;

аутентичность;

3 Обеспечение того, что информационная система ведет себя в нормальном и внештатном режиме так, как запланировано- это..

\*надежность;

точность;

контролируемость;

устойчивость;

доступность;

4. Что, из указанного ниже является принципами информационной безопасности (три варианта):

скрытость;

масштабируемость;

\*системность;

\*законность;

\*открытость алгоритмов;

5. Вирусам изменяющие среду обитания:

черви;

тройские;

\*полиморфные;

макровирусы;

Оценка/баллы	Критерии оценки
<i>Отлично</i>	90-100 % правильных ответов
<i>Хорошо</i>	70-89 % правильных ответов
<i>Удовлетворительно</i>	50-69 % правильных ответов
<i>Неудовлетворительно</i>	49% и меньше правильных ответов

#### 4. Критерии и шкала оценивания результатов обучения по дисциплине (модулю) при проведении промежуточной аттестации

##### 4.1 Критерии и шкала оценивания результатов освоения дисциплины (модуля) с зачетом с оценкой

Если обучающийся набрал зачетное количество баллов согласно установленному диапазону по дисциплине (модулю), то он считается аттестованным с оценкой согласно шкале баллов для определения итоговой оценки:

Оценка	Баллы	Критерии оценивания
<i>Отлично</i>	91 - 100	Набрано зачетное количество балловсогласно установленному диапазону
<i>Хорошо</i>	81 - 90	Набрано зачетное количество балловсогласно установленному диапазону
<i>Удовлетворительно</i>	60 - 80	Набрано зачетное количество балловсогласно установленному диапазону
<i>Неудовлетворительно</i>	менее 60	Зачетное количество согласно установленному диапазону баллов не набрано

## **5. Задания диагностической работы для оценки результатов обучения по дисциплине (модулю) в рамках внутренней и внешней независимой оценки качества образования**

ФОС содержит задания для оценивания знаний, умений и навыков, демонстрирующих уровень сформированности компетенций и индикаторов их достижения в процессе освоения дисциплины (модуля).

Комплект заданий разработан таким образом, чтобы осуществить процедуру оценки каждой компетенции, формируемых дисциплиной (модулем), у обучающегося в письменной форме.

### **Примерные наборы тестовых вопросов**

#### **ВАРИАНТ 1**

1. Информация может составлять коммерческую тайну, если
  - содержится в учредительных документах;
  - \*-к ней нет свободного доступа на законном основании;
  - содержится в бухгалтерских балансах;
2. Правовое обеспечение информационной безопасности- это...
  - документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы;
  - \*-Нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения;
  - широкое использование технических средств защиты информации;
3. Угрозой безопасности автоматизированных банковских систем не является:
  - фишинг;
  - \*аутсорсинг;
  - хакерские атаки;
4. Что, из указанного ниже является принципами информационной безопасности (три варианта):
  - скрытость;
  - масштабируемость;
  - \*системность;
  - \*законность;
  - \*открытость алгоритмов;
5. Вирусам изменяющие среду обитания:
  - черви;
  - тройные;
  - \*полиморфные;
  - макровирусы;

#### **ВАРИАНТ 2**

1. Какие угрозы информационной безопасности являются преднамеренными:
  - неумышленное повреждение каналов связи;
  - некомпетентное использование средств защиты;
  - \*поджог;
2. Что такое несанкционированный доступ?
  - Вход в систему без согласования с руководителем организации;
  - \*доступ в систему в нарушение установленных в системе правил разграничения доступа;
  - Удаление данных без согласования с руководством;
3. Ботнеты- это

\*сеть компьютеров, зараженных вредоносной программой, позволяющей удаленно управлять зараженными компьютерами;  
сеть компьютеров, зараженных блокерами;

сеть компьютеров, распространяющих сетевые черви;

4. Что, из указанного ниже является принципами информационной безопасности (три варианта):

скрытость;

масштабируемость;

\*системность;

\*законность;

\*открытость алгоритмов;

5. Вирусам изменяющие среду обитания:

черви;

троянские;

\*полиморфные;

макровирусы;

### **ВАРИАНТ 3**

1. Какая наиболее яркая черта вируса «сетевой червь»?

распространяется через съемные носители;

\*распространяется по сети;

саморепликация;

2. По числу компьютерных преступлений лидируют:

информационные системы образовательных учреждений;

\*автоматизированные банковские системы;

корпоративные информационные системы в промышленности;

3. Программы, предназначенные для записи информации о нажатиях клавиш клавиатуры в специализированный журнал регистрации(log-файл),который впоследствии изучается установившим программу злоумышленником называются:

malware\$

троянцы-бэкдоры;

\*кейлоггеры;

4. Что, из указанного ниже является принципами информационной безопасности (три варианта):

скрытость;

масштабируемость;

\*системность;

\*законность;

\*открытость алгоритмов;

5. Вирусам изменяющие среду обитания:

черви;

троянские;

\*полиморфные;

макровирусы;

### **ВАРИАНТ 4**

1. К какой главе УК РФ относятся ст.272,ст.273ст.,274 в области информационной безопасности?

27

25

\*28

2. К понятию информационной безопасности не относятся:

- надежность работы компьютеры;
- \*Природоохранные мероприятия;
- сохранность ценных данных;
- 3. К активным угрозам относятся:
  - \*разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или операционной системы;
  - попытка получения информации , циркулирующей в каналах связи, посредством их прослушивания;
  - копирование информации;
- 4. Что, из указанного ниже является принципами информационной безопасности (три варианта):
  - скрытость;
  - масштабируемость;
  - \*системность;
  - \*законность;
  - \*открытость алгоритмов;
- 5. Вирусам изменяющие среду обитания:
  - черви;
  - троянские;
  - \*полиморфные;
  - макровирусы;

#### **ВАРИАНТ 5**

1. В системах дистанционного банковского обслуживания используется следующий протокол, осуществляющий шифрование конфиденциальной информации-
  - http
  - \*https
  - ftp
  - smtp
2. Что такое государственная тайна?
  - сведения о состоянии окружающей среды;
  - все сведения, которые хранятся в государственных базах данных;
  - \*защищаемые государством сведения в различных областях, распространение которых может нанести ущерб безопасности РФ;
3. Не являются коммерческой тайной :
  - сведения о научных разработках;
  - \*сведения, содержащиеся в документах, дающих право заниматься предпринимательской деятельностью;
  - сведения о персонале предприятия;
4. Что, из указанного ниже является принципами информационной безопасности (три варианта):
  - скрытость;
  - масштабируемость;
  - \*системность;
  - \*законность;
  - \*открытость алгоритмов;
5. Вирусам изменяющие среду обитания:
  - черви;
  - троянские;
  - \*полиморфные;
  - макровирусы;

#### **ВАРИАНТ 6**

1. Информационное оружие-это...?  
 комплекс мер направленных на изменение индивидуального и общественного сознания;  
 \*комплекс методов, средств и технологий предназначенных для распространения дезинформации в системе формирования общественного сознания;  
 комплекс нормативно-правовой документации;
- 2 Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена- это...  
 \*конфиденциальность;  
 целостность;  
 доступность;  
 аутентичность;
- 3 Обеспечение того, что информационная система ведет себя в нормальном и внештатном режиме так, как запланировано- это..  
 \*надежность;  
 точность;  
 контролируемость;  
 устойчивость;  
 доступность;
4. Что, из указанного ниже является принципами информационной безопасности (три варианта):  
 скрытость;  
 масштабируемость;  
 \*системность;  
 \*законность;  
 \*открытость алгоритмов;
5. Вирусам изменяющие среду обитания:  
 черви;  
 троянские;  
 \*полиморфные;  
 макровирусы;

### Шкала оценивания комплексного задания

Оценка (баллы)	Критерии оценки
<b>5 «отлично»</b>	5 правильных ответов
<b>4 «хорошо»</b>	4 правильных ответа
<b>3 «удовлетворительно»</b>	3 правильных ответа
<b>2 «неудовлетворительно»</b>	2 и меньше правильных ответа