

Компонент ОПОП 09.03.02 Информационные системы и технологии , направленность (профиль)  
«Информационные системы и технологии искусственного интеллекта»

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 г.

Заведующий кафедрой ИТ

  
подпись

ФИО

Ляш О.И.

## 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-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	ИД-1ОПК-3 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ИД-2ОПК-3 Способен составлять обзоры, аннотации, рефераты, готовить доклады с учетом требований информационной безопасности	принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	навыками подготовки обзоров, аннотаций, составления рефератов, докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	комплект заданий для выполнения практических, лабораторных работ; учет посещаемости; тестовые наборы	Результаты текущего контроля

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

Показатели оценивания компетенций (индикаторов их достижения)	Шкала и критерии оценки 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 основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Выполнены типовые задания с не грубыми ошибками. Выполнены все задания, но не в полном объеме (отсутствуют пояснения, неполные выводы)	Продемонстрированы все основные умения. Выполнены все основные задания с некоторыми погрешностями. Выполнены все задания в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения. Выполнены все 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 МАУ.

Оценка/баллы	Критерии оценивания
<b>Отлично</b>	Задание выполнено полностью и правильно. Отчет по лабораторной/практической работе подготовлен качественно в соответствии с требованиями. Полнота ответов на вопросы преподавателя при защите работы.
<b>Хорошо</b>	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.
<b>Удовлетворительно</b>	Задания выполнены частично с ошибками. Демонстрирует средний уровень выполнения задания на лабораторную/практическую работу. Большинство требований, предъявляемых к заданию, выполнены.
<b>Неудовлетворительно</b>	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 посещаемости занятий

Посещение занятий обучающимися определяется в процентном соотношении

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

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

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

Для дисциплин (модулей), заканчивающихся экзаменом, результат промежуточной аттестации складывается из баллов, набранных в ходе текущего контроля и при проведении экзамена.

Оценка	Критерии оценки ответа на экзамене
<b>Отлично</b>	Обучающийся глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, не затрудняется с ответом при видоизменении вопроса. Владеет специальной терминологией, демонстрирует общую эрудицию в предметной области, использует при ответе ссылки на материал специализированных источников, в том числе на Интернет-ресурсы.
<b>Хорошо</b>	Обучающийся твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, владеет специальной терминологией на достаточном уровне; могут возникнуть затруднения при ответе на уточняющие вопросы по рассматриваемой теме; в целом демонстрирует общую эрудицию в предметной области.
<b>Удовлетворительно</b>	Обучающийся имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, плохо владеет специальной терминологией, допускает существенные ошибки при ответе, недостаточно ориентируется в источниках специализированных знаний.
<b>Неудовлетворительно</b>	Обучающийся не знает значительной части программного материала, допускает существенные ошибки, нарушения логической последовательности в изложении программного материала, не владеет специальной терминологией, не ориентируется в источниках специализированных знаний. Нет ответа на поставленный вопрос.

Оценка, полученная на экзамене, переводится в баллы («5» - 20 баллов, «4» - 15 баллов, «3» - 10 баллов) и суммируется с баллами, набранными в ходе текущего контроля.

<b>Итоговая оценка по</b>	<b>Суммарные баллы</b>	<b>Критерии оценивания</b>
---------------------------	------------------------	----------------------------

дисциплине (модулю)	по дисциплине (модулю), в том числе	
<i>Отлично</i>	91 - 100	Выполнены все контрольные точки текущего контроля на высоком уровне. Экзамен сдан
<i>Хорошо</i>	81-90	Выполнены все контрольные точки текущего контроля. Экзамен сдан
<i>Удовлетворительно</i>	70- 80	Контрольные точки выполнены в неполном объеме. Экзамен сдан
<i>Неудовлетворительно</i>	69 и менее	Контрольные точки не выполнены или не сдан экзамен

### **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.

Содержание комплекта заданий включает тестовые задания

#### **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;
  - тroyанские;
  - \*полиморфные;
  - макровирусы;

#### **ВАРИАНТ 2**

1. Какие угрозы информационной безопасности являются преднамеренными:
  - неумышленное повреждение каналов связи;

некомпетентное использование средств защиты;

\*поджег;

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;

тройские;

\*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\$

тройцы-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;

тройские;

\*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;

тroyанские;

\*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;

тroyанские;

\*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