

**Министерство науки и высшего образования Российской Федерации**  
**Федеральное государственное бюджетное образовательное учреждение высшего**  
**образования**  
**«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ**  
**УНИВЕРСИТЕТ»**

Структурное подразделение «Институт информационных технологий и анализа данных  
(121)»

**УТВЕРЖДЕНА:**

на заседании совета института ИТиАД им. Е.И. Попова  
Протокол №8 от 16 февраля 2026 г.

**Рабочая программа дисциплины**

**«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

---

Направление: 09.04.02 Информационные системы и технологии

---

---

Корпоративные информационные системы. Инновационные методики и платформы

---

---

Квалификация: Магистр

---

---

Форма обучения: очная

---

|                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------|
| Документ подписан простой электронной<br>подписью<br>Составитель программы: Говорков Алексей<br>Сергеевич<br>Дата подписания: 01.06.2026 |
|------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------|
| Документ подписан простой электронной<br>подписью<br>Утвердил и согласовал: Говорков Алексей<br>Сергеевич<br>Дата подписания: 01.06.2026 |
|------------------------------------------------------------------------------------------------------------------------------------------|

Год набора – 2026

Иркутск, 2026 г.

**1 Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы**

**1.1 Дисциплина «Информационная безопасность» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения**

| <b>Код, наименование компетенции</b>                                                                                                                                                                                                                             | <b>Код индикатора компетенции</b> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| ОПК-1 Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте | ОПК-1.6                           |
| ОПК-5 Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем                                                                                                                                   | ОПК-5.6                           |
| ОПК-6 Способен использовать методы и средства системной инженерии в области получения, передачи, хранения, переработки и представления информации посредством информационных технологий                                                                          | ОПК-6.2                           |

**1.2 В результате освоения дисциплины у обучающихся должны быть сформированы**

| <b>Код индикатора</b> | <b>Содержание индикатора</b>                                                                                                                            | <b>Результат обучения</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ОПК-1.6               | Владеет навыками решения нестандартных профессиональных задач с применением информационной безопасности и защиты данных в профессиональной деятельности | <b>Знать</b> Знать четко и правильно дает определения, полно раскрывает содержание понятий, верно использует терминологию, при этом ответ самостоятельный, использованы ранее приобретенные знания.<br><b>Уметь</b> Уметь выполняет все операции, последовательность их выполнения достаточно хорошо продумана, действие в целом осознано.<br><b>Владеть</b> Владеть навыками использования системного и прикладного программного обеспечения, в том числе отечественного производства, для решения задач профессиональной деятельности. |
| ОПК-5.6               | Владеет навыками решения профессиональных задач, с применением информационной безопасности и защиты данных в профессиональной деятельности              | <b>Знать</b> Знать состав, классификацию, особенности функционирования программных средств системного и прикладного назначений, в том числе отечественного производства.<br><b>Уметь</b> Уметь оперировать базовой                                                                                                                                                                                                                                                                                                                       |

|         |                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |                                                                                                                                                  | <p>терминологией в области информационных технологий, информационной безопасности личности, общества и государства, гуманитарных аспектов информационной безопасности.</p> <p><b>Владеть</b> Владеть навыками использования системного и прикладного программного обеспечения, в том числе отечественного производства, для решения задач профессиональной деятельности.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| ОПК-6.2 | <p>Владеет навыками решения профессиональных задач с применением информационной безопасности и защиты данных в профессиональной деятельности</p> | <p><b>Знать</b> Знать сущность и понятие информации, информационной безопасности, их роль в современном обществе, значение для обеспечения объективных потребностей личности общества и государства; психологические аспекты информационной безопасности в современном обществе; угрозы и источники угроз информационной безопасности современного общества.</p> <p><b>Уметь</b> Уметь рационально использовать функциональные возможности программных средств системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.</p> <p><b>Владеть</b> Владеть основными информационными технологиями, базовыми методами выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угроз информационной безопасности.</p> |

## 2 Место дисциплины в структуре ООП

Изучение дисциплины «Информационная безопасность» базируется на результатах освоения следующих дисциплин/практик: «Академическое письмо»

Дисциплина является предшествующей для дисциплин/практик: «Распределенная обработка больших объемов данных»

## 3 Объем дисциплины

Объем дисциплины составляет – 3 ЗЕТ

| Вид учебной работы                                                 | Трудоемкость в академических часах<br>(Один академический час соответствует 45 минутам астрономического часа) |             |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|-------------|
|                                                                    | Всего                                                                                                         | Семестр № 4 |
| Общая трудоемкость дисциплины                                      | 108                                                                                                           | 108         |
| Аудиторные занятия, в том числе:                                   | 48                                                                                                            | 48          |
| лекции                                                             | 24                                                                                                            | 24          |
| лабораторные работы                                                | 0                                                                                                             | 0           |
| практические/семинарские занятия                                   | 24                                                                                                            | 24          |
| Самостоятельная работа (в т.ч. курсовое проектирование)            | 60                                                                                                            | 60          |
| Трудоемкость промежуточной аттестации                              | 0                                                                                                             | 0           |
| Вид промежуточной аттестации<br>(итогового контроля по дисциплине) | Зачет                                                                                                         | Зачет       |

#### 4 Структура и содержание дисциплины

##### 4.1 Сводные данные по содержанию дисциплины

##### Семестр № 4

| №<br>п/п | Наименование<br>раздела и темы<br>дисциплины                                                                     | Виды контактной работы |              |    |              |         |              | СРС |              | Форма<br>текущего<br>контроля |
|----------|------------------------------------------------------------------------------------------------------------------|------------------------|--------------|----|--------------|---------|--------------|-----|--------------|-------------------------------|
|          |                                                                                                                  | Лекции                 |              | ЛР |              | ПЗ(СЕМ) |              |     |              |                               |
|          |                                                                                                                  | №                      | Кол.<br>Час. | №  | Кол.<br>Час. | №       | Кол.<br>Час. | №   | Кол.<br>Час. |                               |
| 1        | 2                                                                                                                | 3                      | 4            | 5  | 6            | 7       | 8            | 9   | 10           | 11                            |
| 1        | Основные<br>понятия и задачи<br>информационной<br>безопасности                                                   | 1                      | 4            |    |              | 1       | 4            | 1   | 10           | Устный<br>опрос               |
| 2        | Основы защиты<br>информации                                                                                      | 2                      | 4            |    |              | 2       | 4            | 1   | 10           | Устный<br>опрос               |
| 3        | Угрозы<br>безопасности<br>защищаемой<br>информации.                                                              | 3                      | 4            |    |              | 3       | 6            | 1   | 10           | Устный<br>опрос               |
| 4        | Методологически<br>е подходы к<br>защите<br>информации                                                           | 4                      | 4            |    |              |         |              | 1   | 5            | Устный<br>опрос               |
| 5        | Понятия<br>юридической<br>ответственности<br>за<br>правонарушения<br>в области<br>информационной<br>безопасности | 5                      | 2            |    |              | 4       | 6            | 1   | 5            | Устный<br>опрос               |
| 6        | Законодательство<br>Российской<br>Федерации о<br>гражданско -<br>правовой                                        | 6                      | 2            |    |              | 5       | 4            | 1   | 10           | Устный<br>опрос               |

|   |                                                                                                                                               |   |    |  |  |  |    |   |    |              |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------|---|----|--|--|--|----|---|----|--------------|
|   | ответственности в сфере инфобезопасности и Законодательство Российской Федерации об административной ответственности в сфере инфобезопасности |   |    |  |  |  |    |   |    |              |
| 7 | Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации)                                         | 7 | 4  |  |  |  |    | 1 | 10 | Устный опрос |
|   | Промежуточная аттестация                                                                                                                      |   |    |  |  |  |    |   |    | Зачет        |
|   | Всего                                                                                                                                         |   | 24 |  |  |  | 24 |   | 60 |              |

#### 4.2 Краткое содержание разделов и тем занятий

##### Семестр № 4

| № | Тема                                                  | Краткое содержание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Основные понятия и задачи информационной безопасности | Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. Понятие «угроза информации». Понятие «риска информационной безопасности». 2 Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от не информированности в области информационной безопасности.                                 |
| 2 | Основы защиты информации                              | Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. 4 Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации. Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности |

|   |                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3 | Угрозы безопасности защищаемой информации.                                                                                                                                                                   | Понятие угрозы безопасности информации<br>Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к информации<br>Уязвимости. Методы оценки уязвимости информации                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 4 | Методологические подходы к защите информации                                                                                                                                                                 | Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 5 | Понятия юридической ответственности за правонарушения в области информационной безопасности                                                                                                                  | 1. Основные документы в области информационной безопасности Российской Федерации 2. Информация как объект правовых отношений 3. Функции, принципы и виды юридической ответственности. 4. Субъективная и объективная стороны юридической ответственности                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 6 | Законодательство Российской Федерации о гражданско - правовой ответственности в сфере инфобезопасности<br>Законодательство Российской Федерации об административной ответственности в сфере инфобезопасности | 1. Общие положения законодательства Российской Федерации о гражданско - правовой ответственности 2. Порядок привлечения несовершеннолетних к гражданско -правовой ответственности за проступки в области информационной безопасности<br>1. Ответственность за проступок в области нарушения авторских прав на лицензионное программное обеспечение 2. Ответственность за проступок – за оскорбления, в том числе в социальных сетях 3. Ответственность за проступок - ложный вызов экстренных служб 4. Ответственность за проступок - пропаганду в Интернете наркотических и психотропных веществ 5. Ответственность за проступок – нарушение установленного законом порядка сбора, хранения, использования или 9 5 4 распространения информации о гражданах (персональные данные) 6. Ответственность за проступок – нарушение правил защиты информации 7. Ответственность за проступок – представление ложных сведений для получения документа, удостоверяющего личность гражданина (паспорта), либо других документов, удостоверяющих личность или гражданство 8. Ответственность за проступок – за подделку документов, штампов, печатей или бланков, их использование, передача, либо сбыт 9. Ответственность за проступок –нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения |

|   |                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   |                                                                                                       | информации                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 7 | Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации) | 1. Ответственность за преступления в области компьютерной информации и применения компьютеров 2. Ответственность за преступления в области присвоения авторства (плагиат) 3. Ответственность за преступления в области нарушения авторских прав на лицензионное программное обеспечение 4. Ответственность за преступления в области мошенничества (обмана) 5. Ответственность за преступления в области нарушения тайны переписки, телефонных переговоров или иных сообщений 6. Ответственность за преступления – за проведение скрытой (негласной) аудиозаписи 7. Ответственность за преступления – за заведомо ложное сообщение о теракте 8. Ответственность за преступления – за неприкосновенности частной жизни (тайна общения и творчества, дневников, личных бумаг) 11 6 5 9. Ответственность за преступления – за мошенничество в сфере компьютерной информации 10. Ответственность за преступления – за незаконное распространение порнографических материалов |

#### 4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

#### 4.4 Перечень практических занятий

##### Семестр № 4

| № | Темы практических (семинарских) занятий                                                                | Кол-во академических часов |
|---|--------------------------------------------------------------------------------------------------------|----------------------------|
| 1 | Основные понятия и задачи информационной безопасности                                                  | 4                          |
| 2 | Основы защиты информации                                                                               | 4                          |
| 3 | Угрозы безопасности защищаемой информации.                                                             | 6                          |
| 4 | Понятия юридической ответственности за правонарушения в области информационной безопасности            | 6                          |
| 5 | Законодательство Российской Федерации о гражданско - правовой ответственности в сфере инфобезопасности | 4                          |

#### 4.5 Самостоятельная работа

##### Семестр № 4

| № | Вид СРС             | Кол-во академических часов |
|---|---------------------|----------------------------|
| 1 | Подготовка к зачёту | 60                         |

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: Кейс-технологии

## **5 Перечень учебно-методического обеспечения дисциплины**

### **5.1 Методические указания для обучающихся по освоению дисциплины**

#### **5.1.1 Методические указания для обучающихся по практическим занятиям**

Практическое занятие — это форма организации учебного процесса, направленная на выработку у обучающихся практических умений для изучения последующих дисциплин (модулей) и для решения профессиональных задач.

Практическое занятие должно проводиться в учебных кабинетах или специально оборудованных помещениях (площадках, полигонах и т.п.). Продолжительность занятия не менее двух академических часов. Необходимыми структурными элементами практического занятия, помимо самостоятельной деятельности студентов, являются инструктаж, проводимый преподавателем, а также анализ и оценка выполненных работ и степени овладения студентами запланированными умениями.

#### **5.1.2 Методические указания для обучающихся по самостоятельной работе:**

Самостоятельная работа - это основа полноценного образования, планируемая и выполняемая работа обучающихся по заданию, и при методическом руководстве преподавателя, но без его непосредственного участия. Цель самостоятельной работы - научить обучающегося осмысленно и самостоятельно работать с учебным материалом, с научной информацией, заложить основы самоорганизации и самовоспитания с тем, чтобы привить умение и стремление в дальнейшем непрерывно повышать свою квалификацию. Самостоятельная работа выполняет ряд важных функций: • развивающая (повышение культуры умственного труда, обогащение интеллектуальных способностей обучающихся); • ориентирующая и стимулирующая (процессу обучения придается ускорение и мотивация); • воспитательная (формируются и развиваются профессиональные качества специалиста); • исследовательская (новый уровень профессионально-творческого мышления); • информационно-обучающая (учебная деятельность обучающихся на аудиторных занятиях). Задачи самостоятельной работы: • систематизация и закрепление полученных теоретических знаний и практических умений обучающихся; • углубление и расширение теоретических знаний; • формирование умения использовать справочную литературу; • развитие познавательных способностей и активности обучающихся: творческой инициативы, самостоятельности, ответственности и организованности; • формирование самостоятельности мышления, способностей к саморазвитию; самосовершенствованию и самореализации; • развитие исследовательских умений.

## **6 Фонд оценочных средств для контроля текущей успеваемости и проведения промежуточной аттестации по дисциплине**

### **6.1 Оценочные средства для проведения текущего контроля**

#### **6.1.1 семестр 4 | Устный опрос**

##### **Описание процедуры.**

Метод контроля, при котором обучающиеся устно отвечают на вопросы преподавателя, излагая изученный материал. Это может быть как беседа, так и рассказ, объяснение или



даже чтение текста. Устный опрос позволяет преподавателю оценить не только знания обучающегося, но и его умение связно излагать мысли, развивать речь и память.

### **Критерии оценивания.**

Решает нестандартные профессиональные задачи с применением знаний о цифровой трансформации. Умеет создавать блок-схемы алгоритмов функционирования программного обеспечения.

## **6.2 Оценочные средства для проведения промежуточной аттестации**

### **6.2.1 Критерии и средства (методы) оценивания индикаторов достижения компетенции в рамках промежуточной аттестации**

| <b>Индикатор достижения компетенции</b> | <b>Критерии оценивания</b>                                                                                                                                                                          | <b>Средства (методы) оценивания промежуточной аттестации</b> |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| ОПК-1.6                                 | Умеет проектировать программное обеспечение для решения прикладных задач управления предприятием.                                                                                                   | Устный опрос                                                 |
| ОПК-5.6                                 | Сформировавшееся систематическое знание методов выявления требований, проецирования их на компоненты подсистемы концептуального проекта системы автоматизации и методов проектирования компонентов. | Устный опрос                                                 |
| ОПК-6.2                                 | Сформировавшееся систематическое знание видов технической документации, международных и российских стандартов; методов составления технической документации                                         | Устный опрос                                                 |

### **6.2.2 Типовые оценочные средства промежуточной аттестации**

#### **6.2.2.1 Семестр 4, Типовые оценочные средства для проведения зачета по дисциплине**

##### **6.2.2.1.1 Описание процедуры**

Формы проведения зачета устное собеседование. Преподаватель может задавать уточняющие вопросы по существу ответа и дополнительные вопросы.

##### Пример задания:

Описание процедуры:

Включает в себя тестовое задание, которое состоит из 10 вопросов.

В каждом вопросе всего один правильный ответ.

Пример задания:

Задание № 1

Вопрос:

Компьютерным вирусом называется:

Выберите один из 4 вариантов ответа:

- 1) Любая программа, созданная на языках низкого уровня
- 2) Небольшая программа, способная к самокопированию, которая может приписывать себя к другим программам
- 3) Файл, содержащий макросы
- 4) Нет правильного ответа

Задание № 2

Вопрос:

Что из нижеперечисленного является одним из способов защиты информации на компьютере?

Выберите один из 6 вариантов ответа:

- 1) защита паролем данных
- 2) дефрагментация жесткого диска
- 3) полное отключение системного блока
- 4) переустановка операционной системы
- 5) нет правильного ответа
- 6) все ответы правильные

Задание № 3

Вопрос:

Сопоставьте вирус и его описание:

Укажите соответствие для всех 4 вариантов ответа:

- 1) перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные объекты
- 2) использует возможности макроязыков, встроенных в офисные пакеты
- 3) маскируется под полезную программу, но выполняют разрушительные действия (например, сбор конфиденциальной информации - паролей)
- 4) вычисляет адреса доступных компьютеров в сети и распространяет по ней свои копии

\_\_\_ Макровирус

\_\_\_ Троян

\_\_\_ Червь

\_\_\_ Стелс-вирус

Задание № 4

Вопрос:

Какие из перечисленных программ являются антивирусами?

Выберите несколько из 5 вариантов ответа:

- 1) Avast
- 2) Nod32
- 3) Scilab
- 4) VirtualBox
- 5) CCleaner

Задание № 5

Вопрос:

Что из указанных вариантов указывает на возможное заражение компьютера вирусами?

Выберите несколько из 5 вариантов ответа:

- 1) Резкое снижение быстродействия компьютера
- 2) исчезновение файлов и папок или искажение их содержимого
- 3) самопроизвольная переустановка программного обеспечения
- 4) не выполняется поиск файлов
- 5) все ответы верны

Задание № 6

Вопрос:

Сопоставьте каждому изображению название антивирусной программы

Укажите соответствие для всех 5 вариантов ответа:

- 1) 360 total security
- 2) Kaspersky Antivirus
- 3) DrWeb
- 4) Comodo
- 5) Avast

—  
—  
—  
—  
—

Задание № 7

Вопрос:

Что такое руткит ?

Выберите один из 5 вариантов ответа:

- 1) вредоносная программа, отслеживающая, какие сайты посещает пользователь
- 2) программа, блокирующая доступ к компьютеру и требующая деньги за разблокировку
- 3) программа для скрытого взятия под контроль взломанной системы
- 4) нет правильного ответа
- 5) все ответы верны

Задание № 8

Вопрос:

Если вирус внедряется в исполняемые файлы и при их запуске активируется, то этот вирус называется...

Выберите один из 4 вариантов ответа:

- 1) Макровирус
- 2) Троян
- 3) Загрузочный вирус
- 4) Файловый вирус

Задание № 9

Вопрос:

К биометрическим способам защиты информации относятся:

Выберите несколько из 5 вариантов ответа:

- 1) идентификация по отпечаткам пальцев
- 2) установка брандмауэра
- 3) идентификация по голосу

- 4) защита паролем
- 5) все ответы верны

#### Задание № 10

Вопрос:

Макровирусы поражают файлы следующих форматов:

Выберите несколько из 7 вариантов ответа:

- 1) .exe
- 2) .raw
- 3) .docx
- 4) .xls
- 5) .dll
- 6) все ответы верны
- 7) нет верных ответов

Критерии оценки:

От 9 и более- оценка «5»

От 8 или ниже- оценка «4»

От 7 или ниже- оценка «3»

Менее 7- оценка «2»\_

#### 6.2.2.1.2 Критерии оценивания

| Зачтено                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Не зачтено                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- систематизированные, глубокие и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы;</li> <li>- точное использование научной терминологии систематически грамотное и логически правильное изложение ответа на вопросы;</li> <li>- безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач;</li> <li>- выраженная способность самостоятельно и творчески решать сложные проблемы и нестандартные ситуации;</li> <li>- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине;</li> <li>- умение ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин.</li> </ul> | <ul style="list-style-type: none"> <li>- фрагментарные знания по дисциплине;</li> <li>- отказ от ответа (выполнения письменной работы);</li> <li>- знание отдельных источников, рекомендованных учебной программой по дисциплине;</li> <li>- неумение использовать научную терминологию;</li> <li>- наличие грубых ошибок;</li> <li>- низкий уровень культуры исполнения заданий;</li> <li>- низкий уровень сформированности заявленных в рабочей программе компетенций.</li> </ul> |

## **7 Основная учебная литература**

1. • Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018. - 88 с.

[Сайт] – URL: нет

## **8 Дополнительная учебная литература и справочная**

1. • Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с.

[Сайт] – URL: нет

2. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.

[Сайт] – URL: нет

## **9 Ресурсы сети Интернет**

1. <http://library.istu.edu/>
2. <https://e.lanbook.com/>

## **10 Профессиональные базы данных**

1. <http://new.fips.ru/>
2. <http://www1.fips.ru/>

## **11 Перечень информационных технологий, лицензионных и свободно распространяемых специализированных программных средств, информационных справочных систем**

1. Свободно распространяемое программное обеспечение Microsoft Windows

## **12 Материально-техническое обеспечение дисциплины**

1. Сервер специал. HP Multiseat 6000 Q9500 500G 6G 31PC Intel Core2 Quad /DVD+RW
2. экран Projecta
3. Блок б/п пит Ippon Smart Winn 1500
4. Проектор TOSHIBA TLP-X3000
5. Доска магнитно-маркерная INDEX настенная ,размер 1x1.8 м
6. Монитор LCD 17 Samsung TCO3