

**Министерство науки и высшего образования РФ**

**ФГБОУ ВО Уральский государственный лесотехнический университет**

**Социально-экономический институт**

*Кафедра интеллектуальных систем*

## **Рабочая программа дисциплины**

включая фонд оценочных средств и методические указания для  
самостоятельной работы обучающихся

---

### **Б1.В.ДЭ.02.02 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

Направление подготовки 09.04.03 «Прикладная информатика»

Направленность (профиль) – " Прикладная информатика в управлении организационными системами "

Квалификация – магистр

Количество зачётных единиц (часов) – 4 (144)

Разработчик



доцент, к.с-х.н. Е.В.Анянова

Рабочая программа утверждена на заседании кафедры интеллектуальных систем  
(протокол № 6 от «01» февраля 2023 года).

Зав. кафедрой  / В.В.Побединский /

Рабочая программа рекомендована к использованию в учебном процессе методической  
комиссией института социально-экономического института  
(протокол № 2 от «02» марта 2023 года).

Председатель методической комиссии СЭИ  / А.В.Чевардин /

Рабочая программа утверждена директором социально-экономического института

Директор СЭИ  / Ю.А.Капустина /

«02» 03 2023 года

## Оглавление

|  |    |
|--|----|
| 1. Общие положения .....   | 4  |
| 2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы .....  | 4  |
| 3. Место дисциплины в структуре образовательной программы .....  | 5  |
| 4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся .....          | 5  |
| 5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов .....  | 6  |
| 5.1. Трудоемкость разделов дисциплины .....  | 6  |
| 5.2. Содержание занятий лекционного типа .....   | 6  |
| 5.3. Темы и формы практических (лабораторных) занятий .....  | 7  |
| 5.4. Детализация самостоятельной работы .....  | 8  |
| 6. Перечень учебно-методического обеспечения по дисциплине .....   | 8  |
| 7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине .....  | 9  |
| 7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы .....   | 9  |
| 7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания .....   | 10 |
| 7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы ..... | 10 |
| 7.4. Соответствие балльной шкалы оценок и уровней сформированных компетенций .....   | 14 |
| 8. Методические указания для самостоятельной работы обучающихся .....  | 14 |
| 9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине .....  | 14 |
| 10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине .....   | 16 |

## 1. Общие положения

Дисциплина «Информационная безопасность» относится к обязательной части (блоку Б1) учебного плана, входящего в состав основной профессиональной образовательной программы высшего образования (ОПОП ВО) направления подготовки 09.04.03 – Прикладная информатика (профиль – Прикладная информатика в управлении организационными системами).

Нормативно-методической базой для разработки рабочей программы учебной дисциплины «Информационные технологии в профессиональной деятельности» являются:

- Федеральный закон РФ от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» с изменениями;

- Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденный приказом Минобрнауки России от 06.04.2021 № 245

- Учебные планы образовательной программы высшего образования направления 09.03.03 – Прикладная информатика (профиль – Цифровая экономика) подготовки бакалавров по очной, заочной, очно-заочной формам обучения, одобренные Ученым советом УГЛТУ (Протокол № 03 от 16.03.2023) и утвержденного ректором УГЛТУ (16.03.2023).

- Приказ Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 г. N 896н с изменением, внесенным приказом Министерства труда и социальной защиты Российской Федерации от 12 декабря 2016 г. N 727н, об утверждении профессионального стандарта 06.015 «Специалист по информационным системам».

- Приказ Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 г. N 893н с изменением, внесенным приказом Министерства труда и социальной защиты Российской Федерации от 12 декабря 2016 г. N 727н об утверждении профессионального стандарта 06.016 «Руководитель проектов в области информационных систем».

- Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 09.04.03 «Прикладная информатика» (уровень высшего образования магистратура), утвержденный приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 916.

Обучение по образовательной программе 09.04.03 – Прикладная информатика (профиль – Прикладная информатика в управлении организационными системами) осуществляется на русском языке.

## 2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Планируемыми результатами обучения по дисциплине являются знания, умения, владения и/или опыт деятельности, характеризующие этапы/уровни формирования компетенций и обеспечивающие достижение планируемых результатов освоения образовательной программы в целом.

**Целью дисциплины** является ознакомление обучающихся с угрозами информационной безопасности, методами и средствами защиты информации.

### **Задачи дисциплины:**

- формирование у обучающихся системы знаний по основным положениям теории информации, информационной безопасности и стандартами шифрования;

- изучение математических основ защиты информации; методов, средств и инструментов шифрования, применяемых в сфере информационных технологий и бизнеса;
- приобретение навыков работы с методами шифрования и криптоанализа;
- формирование представлений об информационной безопасности, включая аппаратную часть и математическое обеспечение.

**Процесс изучения дисциплины направлен на формирование следующих компетенции:**

**ПК-1.**Способен использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС.

**ПК-8.** Способен принимать эффективные управленческие решения по управлению ИТ-проектами, стратегией ИТ в условиях неопределенности и риска.

**В результате освоения дисциплины обучающийся должен:**

**знать:** основные виды угроз безопасности информации; правила защиты информации; методы и средства защиты информации; основы шифрования и криптографии;

**уметь:** использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования; уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач; оперативно реагировать на различные угрозы информационной безопасности, в том числе при использовании компьютерных программ для тестирования ИС.

**владеть:** способами повышения сохранности информации; методами защиты информации; технологиями шифрования и парольной защитой операционной системы; навыками решения задач криптоанализа и шифрования; обнаружения сетевых проникновений, применения, установки и настройки антивирусных систем и систем распознавания угроз и атак.

### 3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» реализуется в рамках блока Б1.В «Дисциплины (модули)» части, формируемой участниками образовательных отношений учебного плана, что означает формирование в процессе обучения у бакалавра основных профессиональных знаний и компетенций в рамках выбранного направления подготовки. Освоение дисциплины «Информационная безопасность» опирается на знания, умения и компетенции, приобретённые в процессе изучения обеспечивающих дисциплин. В свою очередь, освоение дисциплины «Информационная безопасность» позволяет обучающимся быть подготовленными к изучению обеспечиваемых дисциплин (см. табл.). Указанные связи дисциплины дают обучающемуся системное представление о комплексе изучаемых дисциплин в соответствии с ФГОС ВО, что обеспечивает требуемый теоретический уровень и практическую направленность в системе обучения и будущей деятельности выпускника.

Перечень обеспечивающих, сопутствующих и обеспечиваемых дисциплин

| Обеспечивающие                                | Сопутствующие                          | Обеспечиваемые  |
|---|--|---|
| Правовое регулирование в информационной сфере | Современные коммуникативные технологии | Автоматизированные интегрированные системы управления |
|   |  | Выпускная квалификационная работа                     |

Указанные связи дисциплины дают обучающемуся системное представление о комплексе изучаемых дисциплин в соответствии с ФГОС ВО, что обеспечивает требуемый теоретический уровень и практическую направленность в системе обучения и будущей деятельности выпускника.

**4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся**

Общая трудоемкость дисциплины

| Вид учебной работы                          | Всего академических часов |                        |                        |
|---|---------------------------|------------------------|------------------------|
|   | очная форма               | заочная форма          | очно-заочная форма     |
| <b>Контактная работа с преподавателем*:</b> | <b>18,25</b>              | <b>12,4</b>            | <b>36,25</b>           |
| лекции (Л)                                  | 6                         | 6                      | 18                     |
| лабораторные работы (ЛР)                    | 12                        | 6                      | 18                     |
| иные виды контактной работы                 | 0,25                      | 0,40                   | 0,25                   |
| <b>Самостоятельная работа обучающихся:</b>  | <b>125,75</b>             | <b>131,6</b>           | <b>107,75</b>          |
| изучение теоретического курса               | 106                       | 116                    | 94                     |
| подготовка к текущему контролю              | 8                         | 8                      | 10                     |
| контрольная работа                          | -                         | 4                      | -                      |
| подготовка к промежуточной аттестации       | 11,75                     | 3,6                    | 3,75                   |
| <b>Вид промежуточной аттестации:</b>        | <b>Зачет с оценкой</b>    | <b>Зачет с оценкой</b> | <b>Зачет с оценкой</b> |
| Общая трудоемкость, з.е./ часы              | <b>4/144</b>              | <b>4/144</b>           | <b>4/144</b>           |

\*Контактная работа обучающихся с преподавателем, в том числе с применением дистанционных образовательных технологий, включает занятия лекционного типа, и (или) занятия семинарского типа, лабораторные занятия, и (или) групповые консультации, и (или) индивидуальную работу обучающегося с преподавателем, а также аттестационные испытания промежуточной аттестации. Контактная работа может включать иные виды учебной деятельности, предусматривающие групповую и индивидуальную работу обучающихся с преподавателем. Часы контактной работы определяются Положением об организации и проведении контактной работы при реализации образовательных программ высшего образования, утвержденным Ученым советом УГЛУ от 25 февраля 2020 года.

**5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов**

**5.1. Трудоемкость разделов дисциплины**

**очная форма обучения**

| № п/п | Наименование раздела (темы) дисциплины  | ЛЗ       | ЛР       | Всего контактной работы | Самостоятельная работа |
|-------|---|----------|----------|-------------------------|------------------------|
| 1     | <b>Раздел 1. Основные составляющие информационной безопасности</b>  | <b>1</b> | <b>2</b> | <b>3</b>                | <b>22</b>              |
| 1.1   | Тема 1. Понятие информационной безопасности, ее основные составляющие   | 0,5      | 1        | 1,5                     | 10                     |
| 1.2   | Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность                                    | 0,5      | 1        | 1,5                     | 12                     |
| 2     | <b>Раздел 2. Уровни информационной безопасности</b>   | <b>2</b> | <b>4</b> | <b>6</b>                | <b>22</b>              |
| 2.1   | Тема 3. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности | 1        | 1        | 2                       | 5                      |
| 2.2   | Тема 4. Административный уровень информационной безопасности  | 0,5      | 1        | 1,5                     | 6                      |
| 2.3   | Тема 5. Процедурный уровень информационной безопасности. Управление рисками   | 0,5      | 2        | 2,5                     | 11                     |
| 3     | <b>Раздел 3. Программно-технические меры</b>  | <b>3</b> | <b>6</b> | <b>9</b>                | <b>70</b>              |
| 3.1   | Тема 6. Основные программно-технические меры  | 0,5      | 0,5      | 1                       | 10                     |
| 3.2   | Тема 7. Идентификация и аутентификация,   | 0,5      | 0,5      | 1                       | 10                     |

| № п/п                    | Наименование раздела (темы) дисциплины  | ЛЗ         | ЛР        | Всего контактной работы | Самостоятельная работа |
|--------------------------|---|------------|-----------|-------------------------|------------------------|
|                          | управление доступом   |            |           |                         |                        |
| 3.3                      | Тема 8. Моделирование и аудит, шифрование, контроль целостности. Протоколирование и аудит | 0,5        | 1         | 1,5                     | 10                     |
| 3.4                      | Тема 9. Экранирование, анализ защищенности.   | 0,5        | 1         | 1,5                     | 10                     |
| 3.5                      | Тема 10. Обеспечение высокой доступности  | 0,5        | 1         | 1,5                     | 10                     |
| 3.6                      | Тема 11. Туннелирование и управление  | 0,5        | 1         | 1,5                     | 10                     |
| 3.7                      | Тема 12. Криптографические методы защиты информации                                       | -          | 1         | 1                       | 10                     |
| Итого по разделам        |   | <b>6</b>   | <b>12</b> | <b>34</b>               | <b>114</b>             |
| Промежуточная аттестация |   | <b>x</b>   | <b>x</b>  | <b>0,25</b>             | <b>11,75</b>           |
| <b>Всего часов</b>       |   | <b>144</b> |           |                         |                        |

### заочная форма обучения

| № п/п                    | Наименование раздела (темы) дисциплины  | ЛЗ         | ЛР       | Всего контактной работы | Самостоятельная работа |
|--------------------------|---|------------|----------|-------------------------|------------------------|
| 1                        | <b>Раздел 1. Основные составляющие информационной безопасности</b>  | <b>2</b>   | <b>2</b> | <b>4</b>                | <b>10</b>              |
| 1.1                      | Тема 1. Понятие информационной безопасности, ее основные составляющие   | 1          | 1        | 2                       | 5                      |
| 1.2                      | Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность                                    | 1          | 1        | 2                       | 5                      |
| 2                        | <b>Раздел 2. Уровни информационной безопасности</b>   | <b>3</b>   | <b>4</b> | <b>9</b>                | <b>18</b>              |
| 2.1                      | Тема 3. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности | 1          | 2        | 3                       | 6                      |
| 2.2                      | Тема 4. Административный уровень информационной безопасности  | 1          | 2        | 3                       | 6                      |
| 2.3                      | Тема 5. Процедурный уровень информационной безопасности. Управление рисками   | 1          | -        | 1                       | 6                      |
| 3                        | <b>Раздел 3. Программно-технические меры</b>  | <b>1</b>   | <b>-</b> | <b>1</b>                | <b>96</b>              |
| 3.1                      | Тема 6. Основные программно-технические меры  | 1          | -        | 1                       | 10                     |
| 3.2                      | Тема 7. Идентификация и аутентификация, управление доступом   | -          | -        | -                       | 10                     |
| 3.3                      | Тема 8. Моделирование и аудит, шифрование, контроль целостности. Протоколирование и аудит                                   | -          | -        | -                       | 10                     |
| 3.4                      | Тема 9. Экранирование, анализ защищенности.   | -          | -        | -                       | 10                     |
| 3.5                      | Тема 10. Обеспечение высокой доступности  | -          | -        | -                       | 20                     |
| 3.6                      | Тема 11. Туннелирование и управление  | -          | -        | -                       | 20                     |
| 3.7                      | Тема 12. Криптографические методы защиты информации   | -          | -        | -                       | 16                     |
| Итого по разделам        |   | <b>6</b>   | <b>6</b> | <b>10</b>               | <b>124</b>             |
| Контрольная работа       |   |            |          | <b>0,15</b>             | <b>4</b>               |
| Промежуточная аттестация |   | <b>x</b>   | <b>x</b> | <b>0,25</b>             | <b>3,6</b>             |
| <b>Всего часов</b>       |   | <b>180</b> |          |                         |                        |

### Очно-заочная форма обучения

| № п/п | Наименование раздела (темы) дисциплины                             | ЛЗ       | ЛР       | Всего контактной работы | Самостоятельная работа |
|-------|--|----------|----------|-------------------------|------------------------|
| 1     | <b>Раздел 1. Основные составляющие информационной безопасности</b> | <b>2</b> | <b>2</b> | <b>4</b>                | <b>16</b>              |
| 1.1   | Тема 1. Понятие информационной безопасности,                       | 1        | 1        | 2                       | 8                      |

| № п/п                    | Наименование раздела (темы) дисциплины  | ЛЗ         | ЛР        | Всего контактной работы | Самостоятельная работа |
|--------------------------|---|------------|-----------|-------------------------|------------------------|
|                          | ее основные составляющие  |            |           |                         |                        |
| 1.2                      | Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность                                    | 1          | 1         | 2                       | 8                      |
| 2                        | Раздел 2. Уровни информационной безопасности  | <b>6</b>   | <b>6</b>  | <b>12</b>               | <b>18</b>              |
| 2.1                      | Тема 3. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности | 2          | 2         | 4                       | 6                      |
| 2.2                      | Тема 4. Административный уровень информационной безопасности  | 2          | 2         | 4                       | 6                      |
| 2.3                      | Тема 5. Процедурный уровень информационной безопасности. Управление рисками   | 2          | 2         | 4                       | 6                      |
| 3                        | Раздел 3. Программно-технические меры   | <b>10</b>  | <b>10</b> | <b>20</b>               | <b>70</b>              |
| 3.1                      | Тема 6. Основные программно-технические меры  | 1          | 1         | 2                       | 10                     |
| 3.2                      | Тема 7. Идентификация и аутентификация, управление доступом   | 1          | 1         | 2                       | 10                     |
| 3.3                      | Тема 8. Моделирование и аудит, шифрование, контроль целостности. Протоколирование и аудит                                   | 1          | 1         | 2                       | 10                     |
| 3.4                      | Тема 9. Экранирование, анализ защищенности.   | 2          | 2         | 4                       | 10                     |
| 3.5                      | Тема 10. Обеспечение высокой доступности  | 2          | 2         | 4                       | 10                     |
| 3.6                      | Тема 11. Туннелирование и управление  | 2          | 2         | 4                       | 10                     |
| 3.7                      | Тема 12. Криптографические методы защиты информации   | 1          | 1         | 2                       | 10                     |
| Итого по разделам        |   | <b>18</b>  | <b>18</b> | <b>36</b>               | <b>104</b>             |
| Промежуточная аттестация |   | <b>x</b>   | <b>x</b>  | <b>0,25</b>             | <b>3,75</b>            |
| <b>Всего часов</b>       |   | <b>180</b> |           |                         |                        |

## 5.2. Содержание занятий лекционного типа

### Раздел 1. Основные составляющие информационной безопасности.

#### Тема 1. Понятие информационной безопасности, ее основные составляющие

Понятие информационной безопасности; Основные составляющие информационной безопасности; Важность и сложность проблемы информационной безопасности Основные определения и критерии классификации угроз. Некоторые примеры угроз доступности; Вредоносное программное обеспечение.

#### Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность

О необходимости объектно-ориентированного подхода к информационной безопасности; Основные понятия объектно-ориентированного подхода; Применение объектно-ориентированного подхода к рассмотрению защищаемых систем; Недостатки традиционного подхода к информационной безопасности с объектной точки зрения.

### Раздел 2. Уровни информационной безопасности

#### Тема 3. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности

Важность законодательного уровня информационной безопасности; Обзор российского законодательства в области информационной безопасности; Правовые акты общего назначения. Стандарты и спецификации в области информационной безопасности: основные понятия, механизмы безопасности, классы безопасности, информационная безопасность распределенных систем. Рекомендации X.800. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий». Гармонизированные критерии Европейских стран. Руководящие документы Федеральной службы по техническому и экспортному контролю Российской Федерации.



#### **Тема 4. Административный уровень информационной безопасности**

Основные понятия. Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом систем.

#### **Тема 5. Процедурный уровень информационной безопасности. Управление рисками**

Основные классы мер процедурного уровня; Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.

Управление рисками: основные понятия. Подготовительные этапы управления рисками. Подготовительные этапы управления рисками. Основные этапы управления рисками.

### **Раздел 3. Программно-технические меры**

#### **Тема 6. Основные программно-технические меры**

Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность.

#### **Тема 7. Идентификация и аутентификация, управление доступом**

Идентификация и аутентификация. Парольная аутентификация. Одноразовые пароли. Сервер аутентификации Kerberos. Идентификация/аутентификация с помощью биометрических данных. Управление доступом. Ролевое управление доступом. Управление доступом в Java-среде. Возможный подход к управлению доступом в распределенной объектной среде.

#### **Тема 8. Моделирование и аудит, шифрование, контроль целостности. Протоколирование и аудит**

Основные понятия. Активный аудит. Функциональные компоненты и архитектура. Шифрование. Контроль целостности. Цифровые сертификаты.

#### **Тема 9. Экранирование, анализ защищенности.**

Экранирование. Основные понятия. Архитектурные аспекты. Классификация межсетевых экранов. Анализ защищенности.

#### **Тема 10. Обеспечение высокой доступности**

Доступность. Основные понятия. Основы мер обеспечения высокой доступности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости. Программное обеспечение промежуточного слоя. Обеспечение обслуживаемости.

#### **Тема 11. Туннелирование и управление**

Туннелирование. Управление. Основные понятия. Возможности типичных систем.

#### **Тема 12. Криптографические методы защиты информации.**

История криптографии. Шифры и их свойства. Системы шифрования с открытыми ключами. Классификация алгоритмов шифрования информации. Симметричные и асимметричные криптосистемы. Сеть Фештеля, стандарт AES. Методы рандомизации сообщений. Архивация - алгоритмы Хаффмана, Лемпеля-Зива. Криптографические хеш-функции. Алгоритмы RSA. Электронные цифровые подписи. Обмен ключами по алгоритму Диффи-Хеллмана. Криптографические стандарты.

### **5.3. Темы и формы занятий семинарского типа (лабораторные работы)**

Учебный планом по дисциплине предусмотрены лабораторные работы

| № п/п   | Наименование занятий семинарского типа (практических занятий)         | Форма проведения занятия | Трудоёмкость, час. |         |              |
|---|---|--------------------------|--------------------|---------|--------------|
|   |   |                          | очная              | заочная | очно-заочная |
| Раздел 1. Основные составляющие информационной безопасности |   |                          |                    |         |              |
| 1.  | Тема 1. Понятие информационной безопасности, ее основные составляющие | лабораторные работы      | 1                  | 1       | 1            |

| № п/п  | Наименование занятий семинарского типа (практических занятий)   | Форма проведения занятия | Трудоёмкость, час. |         |              |
|--|---|--------------------------|--------------------|---------|--------------|
|  |   |                          | очная              | заочная | очно-заочная |
| 2.   | Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность                                    | лабораторные работы      | 1                  | 1       | 1            |
| Раздел 2. Уровни информационной безопасности |   |                          |                    |         |              |
| 3.   | Тема 3. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности | лабораторные работы      | 1                  | 2       | 2            |
| 4.   | Тема 4. Административный уровень информационной безопасности  | лабораторные работы      | 1                  | 2       | 2            |
| 5.   | Тема 5. Процедурный уровень информационной безопасности. Управление рисками   | лабораторные работы      | 2                  |         | 2            |
| Раздел 3. Программно-технические меры        |   |                          |                    |         |              |
| 6.   | Тема 6. Основные программно-технические меры  | лабораторные работы      | 0,5                |         | 1            |
| 7.   | Тема 7. Идентификация и аутентификация, управление доступом   | лабораторные работы      | 0,5                |         | 1            |
| 8.   | Тема 8. Моделирование и аудит, шифрование, контроль целостности. Протоколирование и аудит                                   | лабораторные работы      | 1                  |         | 1            |
| 9.   | Тема 9. Экранирование, анализ защищенности.   | лабораторные работы      | 1                  |         | 2            |
| 10.  | Тема 10. Обеспечение высокой доступности  | лабораторные работы      | 1                  |         | 2            |
| 11.  | Тема 11. Туннелирование и управление  | лабораторные работы      | 1                  |         | 2            |
| 12.  | Тема 12. Криптографические методы защиты информации   | лабораторные работы      | 1                  |         | 1            |
| Всего часов                                  |   |                          | 12                 | 6       | 18           |

#### 5.4 Детализация самостоятельной работы

| № п/п   | Наименование занятий семинарского типа (практических занятий)         | Вид самостоятельной работы   | Трудоёмкость, час.   |         |              |
|---|---|--|----------------------|---------|--------------|
|   |   |  | очная форма обучения | заочная | Очно-заочная |
| Раздел 1. Основные составляющие информационной безопасности |   |  |                      |         |              |
| 1   | Тема 1. Понятие информационной безопасности, ее основные составляющие | Изучение теоретического курса (чтение конспекта лекций, специальной литературы)<br>Подготовка к текущему контролю задания в тестовой форме в режиме электронной информационной среды | 10                   | 5       | 8            |

| № п/п  | Наименование занятий семинарского типа (практических занятий)   | Вид самостоятельной работы   | Трудоёмкость, час.   |         |              |
|--|---|--|----------------------|---------|--------------|
|  |   |  | очная форма обучения | заочная | Очно-заочная |
| 2  | Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность                                    | Изучение теоретического курса (чтение конспекта лекций, специальной литературы)<br>Подготовка к текущему контролю задания в тестовой форме в режиме электронной информационной среды | 12                   | 5       | 8            |
| Раздел 2. Уровни информационной безопасности |   |  |                      |         |              |
| 3  | Тема 3. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности | Изучение теоретического курса (чтение конспекта лекций, специальной литературы)<br>Подготовка к текущему контролю задания в тестовой форме в режиме электронной информационной среды | 5                    | 6       | 6            |
| 4  | Тема 4. Административный уровень информационной безопасности  | Изучение теоретического курса (чтение конспекта лекций, специальной литературы)<br>Подготовка к текущему контролю задания в тестовой форме в режиме электронной информационной среды | 6                    | 6       | 6            |
| 5  | Тема 5. Процедурный уровень информационной безопасности. Управление рисками   | Изучение теоретического курса (чтение конспекта лекций, специальной литературы)<br>Подготовка к текущему контролю задания в тестовой форме в режиме электронной информационной среды | 11                   | 6       | 6            |
| Раздел 3. Программно-технические меры        |   |  |                      |         |              |
| 6  | Тема 6. Основные программно-технические меры  | Изучение теоретического курса (чтение конспекта лекций, специальной литературы)<br>Подготовка к текущему контролю задания в тестовой форме в режиме электронной информационной среды | 10                   | 10      | 10           |
| 7  | Тема 7. Идентификация и аутентификация, управление доступом   | Изучение теоретического курса (чтение конспекта лекций, специальной литературы)<br>Подготовка к текущему контролю задания в тестовой форме в режиме электронной информационной среды | 10                   | 10      | 10           |
| 8  | Тема 8. Моделирование и аудит, шифрование, контроль целостности. Протоколирование и аудит                                   | Изучение теоретического курса (чтение конспекта лекций, специальной литературы)<br>Подготовка к текущему контролю задания в тестовой форме в режиме электронной информационной среды | 10                   | 10      | 10           |
| 9  | Тема 9. Экранирование, анализ защищенности  | Изучение теоретического курса (чтение конспекта лекций, специальной литературы)<br>Подготовка к текущему контролю  | 10                   | 10      | 10           |

| № п/п                           | Наименование занятий семинарского типа (практических занятий) | Вид самостоятельной работы   | Трудоёмкость, час.   |              |               |
|---------------------------------|---|--|----------------------|--------------|---------------|
|                                 |   |  | очная форма обучения | заочная      | Очно-заочная  |
|                                 |   | задания в тестовой форме в режиме электронной информационной среды   |                      |              |               |
| 10                              | Тема 10. Обеспечение высокой доступности                      | Изучение теоретического курса (чтение конспекта лекций, специальной литературы)<br>Подготовка к текущему контролю задания в тестовой форме в режиме электронной информационной среды | 10                   | 20           | 10            |
| 11                              | Тема 11. Туннелирование и управление                          | Изучение теоретического курса (чтение конспекта лекций, специальной литературы)<br>Подготовка к текущему контролю задания в тестовой форме в режиме электронной информационной среды | 10                   | 20           | 10            |
| 12                              | Тема 12. Криптографические методы защиты информации           | Изучение теоретического курса (чтение конспекта лекций, специальной литературы)<br>Подготовка к текущему контролю задания в тестовой форме в режиме электронной информационной среды | 10                   | 16           | 10            |
| <b>Итого по разделам</b>        |   |  | <b>114</b>           | <b>124</b>   | <b>104</b>    |
| <b>Промежуточная аттестация</b> |   |  | <b>11,75</b>         | <b>3,75</b>  | <b>3,75</b>   |
| <b>Всего часов</b>              |   |  | <b>125,75</b>        | <b>131,6</b> | <b>107,75</b> |

## 6. Перечень учебно-методического обеспечения по дисциплине

### Основная и дополнительная литература

| № п/п                              | Автор, наименование   | Год издания | Примечание  |
|------------------------------------|---|-------------|---|
| <b>Основная учебная литература</b> |   |             |   |
| 1                                  | Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : НГТУ, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/152227">https://e.lanbook.com/book/152227</a> .— Режим доступа: для авториз. пользователей.   | 2019        | Полнотекстовый доступ при входе по логину и паролю* |
| 2                                  | Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки информации : учебное пособие : [16+] / А. А. Сидак, В. В. Василенко, С. В. Рыженко ; Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова. – Москва : Директ-Медиа, 2022. – 128 с. : ил., табл. – Режим доступа: по подписке. – URL: <a href="https://biblioclub.ru/index.php?page=book&amp;id=694670">https://biblioclub.ru/index.php?page=book&amp;id=694670</a> | 2022        | Полнотекстовый доступ при входе по логину и паролю* |
| 3                                  | Гулятьева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гулятьева. — Новосибирск : НГТУ, 2018. — 79 с. — ISBN 978-5-7782-3640-0. —  | 2018        | Полнотекстовый доступ при входе по логину и паролю* |

|  |  |      |   |
|--|--|------|---|
|  | Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/118233">https://e.lanbook.com/book/118233</a> . — Режим доступа: для авториз. пользователей.   |      |   |
| <b>Дополнительная учебная литература</b> |  |      |   |
| 4  | Информационная безопасность и защита информации : учебное пособие / А. С. Минзов, С. В. Бобылева, П. А. Осипов, А. А. Попов. — Дубна : Государственный университет «Дубна», 2020. — 85 с. — ISBN 978-5-89847-608-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/154490">https://e.lanbook.com/book/154490</a> . — Режим доступа: для авториз. пользователей. | 2020 | Полнотекстовый доступ при входе по логину и паролю* |
| 5  | Защита компьютерной информации : учебное пособие / Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский, О. В. Скулябина. — Санкт-Петербург : БГТУ "Военмех" им. Д.Ф. Устинова, 2019. — 146 с. — ISBN 978-5-907054-82-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/157086">https://e.lanbook.com/book/157086</a> . — Режим доступа: для авториз. пользователей. | 2019 | Полнотекстовый доступ при входе по логину и паролю* |

\*- Прежде чем пройти по ссылке, необходимо войти в систему

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий.

### **Электронные библиотечные системы**

Каждый обучающийся обеспечен доступом к электронной библиотечной системе УГЛУТУ (<http://lib.usfeu.ru/>), ЭБС Издательства Лань (<http://e.lanbook.com/>), ЭБС Университетская библиотека онлайн (<http://biblioclub.ru/>), электронная образовательная система «Образовательная платформа ЮРАЙТ (<https://urait.ru/?=>), универсальная база данных East View (ООО «ИВИС») (<http://www.ivis.ru/>), содержащих издания по основным изучаемым дисциплинам и сформированных по согласованию с правообладателями учебной и учебно-методической литературы. Договоры с ЭБС заключаются университетом ежегодно.

### **Справочные и информационные системы**

1. Справочная правовая система «КонсультантПлюс» (<http://www.consultant.ru/>). Договор заключается университетом ежегодно.
2. Справочно-правовая система «Система ГАРАНТ» (<http://www.garant.ru/>). Доступ свободный.
3. Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат. ВУЗ» (<https://www.antiplagiat.ru/>). Договор заключается университетом ежегодно.
4. Информационная система 1С: ИТС (<http://its.1c.ru/>). Доступ свободный

### **Профессиональные базы данных**

1. Федеральная служба государственной статистики. Официальная статистика (<http://www.gks.ru/>). Доступ свободный.
2. Научная электронная библиотека eLibrary (<http://elibrary.ru/>). Доступ свободный.
3. Экономический портал (<https://institutiones.com/>). Доступ свободный.
4. Информационная система РБК (<https://ekb.rbc.ru/>). Доступ свободный.
5. Официальный интернет-портал правовой информации (<http://pravo.gov.ru/>). Доступ свободный.

6. База полнотекстовых и библиографических описаний книг и периодических изданий (<http://www.ivis.ru/products/udbs.htm>). Доступ свободный.
7. ГлавбухСтуденты: Образование и карьера (<http://student.1gl.ru/>). Доступ свободный.
8. Сайт Центрального банка РФ: официальный сайт Центрального банка Российской Федерации (режим доступа: <https://cbr.ru>). Доступ свободный.

### Нормативно-правовые акты

1. Конституция РФ: официальный текст
2. Гражданский кодекс РФ. Утв. 30 ноября 1994 года № 51-ФЗ (в последней ред.)
3. Федеральный закон «О банках и банковской деятельности». Утв. 02 декабря 1990 г. № 395-1 (в последней ред.)
4. Федеральный закон «О Центральном банке Российской Федерации (Банке России)». Утв. 10 июля 2002 г. № 86-ФЗ (в последней ред.).

### 7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

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

| Формируемые компетенции  | Вид и форма контроля   |
|--|--|
| ПК-1. Способен использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС. | <b>Промежуточный контроль:</b> контрольные вопросы к зачету с оценкой;<br><b>Текущий контроль:</b> лабораторные работы, тестирование, подготовка рефератов, контрольная работа для заочной формы обучения. |
| ПК-8. Способен принимать эффективные управленческие решения по управлению ИТ-проектами, стратегией ИТ в условиях неопределенности и риска.       | <b>Промежуточный контроль:</b> контрольные вопросы к зачету с оценкой;<br><b>Текущий контроль:</b> лабораторные работы, тестирование, подготовка рефератов, контрольная работа для заочной формы обучения. |

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

##### Критерии оценивания устного ответа на контрольные вопросы зачета с оценкой (промежуточный контроль формирования компетенций ПК-1, ПК-8):

*зачтено (отлично)* - дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком в терминах науки, показана способность быстро реагировать на уточняющие вопросы;

*зачтено (хорошо)* - дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен в терминах науки.

Однако допущены незначительные ошибки или недочеты, исправленные магистрантом с помощью «наводящих» вопросов;

*зачтено (удовлетворительно)* - дан неполный ответ, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, теорий, явлений, вследствие непонимания магистрантом их существенных и несущественных признаков и связей. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщенных знаний не показано. Речевое оформление требует поправок, коррекции;

*зачтено (неудовлетворительно)* - магистрант демонстрирует незнание теоретических основ предмета, не умеет делать аргументированные выводы и приводить примеры, показывает слабое владение монологической речью, не владеет терминологией, проявляет отсутствие логичности и последовательности изложения, делает ошибки, которые не может исправить, даже при коррекции преподавателем, отказывается отвечать на занятии.

### **Критерии оценивания выполнения заданий в тестовой форме (текущий контроль формирования компетенций ПК-1, ПК-8)**

По итогам выполнения тестовых заданий оценка производится по четырехбалльной шкале. При правильных ответах на:

86-100% заданий – оценка *«отлично»*;

71-85% заданий – оценка *«хорошо»*;

51-70% заданий – оценка *«удовлетворительно»*;

менее 51% - оценка *«неудовлетворительно»*.

### **Критерии оценивания рефератов (текущий контроль формирования компетенций ПК-1, ПК- 8):**

*отлично*: работа выполнена в соответствии с требованиями, выбранная тема раскрыта полностью, материал актуален и достаточен, магистрант четко и без ошибок ответил на все контрольные вопросы.

*хорошо*: работа выполнена в соответствии с требованиями, выбранная тема раскрыта, материал актуален, магистрант ответил на все контрольные вопросы с замечаниями.

*удовлетворительно*: работа выполнена в соответствии с требованиями, выбранная тема частично раскрыта, по актуальности доклада есть замечания, магистрант ответил на все контрольные вопросы с замечаниями.

*неудовлетворительно*: магистрант не подготовил работу или подготовил работу, не отвечающую требованиям, ответил на контрольные вопросы с ошибками или не ответил на конкретные вопросы.

### **Критерии оценивания контрольной работы для заочной формы обучения (текущий контроль формирования компетенций ПК-1, ПК- 8):**

*отлично*: в контрольной работе выполнены все задания в соответствии с требуемой структурой и требованиями, все задания решены верно и полностью, её материал научно обоснован и достаточен, при защите магистрант четко и без ошибок ответил на все контрольные вопросы;

*хорошо*: в контрольной работе выполнены все задания в соответствии с требуемой структурой и требованиями, материал актуален, при защите магистрант ответил на все контрольные вопросы с замечаниями.

*удовлетворительно*: в контрольной работе выполнены не все задания в соответствии с требуемой структурой и требованиями, по актуальности доклада есть замечания, магистрант ответил не на все контрольные вопросы с замечаниями.

*неудовлетворительно*: магистрант не выполнил ни одного задания или подготовил работу, не отвечающую требованиям, ответил на контрольные вопросы с ошибками или не ответил на конкретные вопросы.

### **Критерии оценивания лабораторных работ (текущий контроль формирования компетенций ПК-1, ПК- 8):**

*отлично:* выполнены все работы, магистрант четко и без ошибок ответил на все контрольные вопросы.

*хорошо:* выполнены все работы, магистрант с небольшими ошибками ответил на все контрольные вопросы.

*удовлетворительно:* выполнены все работы с замечаниями, магистрант ответил на все контрольные вопросы с замечаниями.

*неудовлетворительно:* магистрант не выполнил или выполнил неправильно задания, ответил на контрольные вопросы с ошибками или не ответил на конкретные вопросы.

### **7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы**

#### **Контрольные вопросы к зачету с оценкой**

1. Какие вы знаете методы криптографической защиты файлов?
2. В чем преимущества и недостатки одноалфавитных методов?
3. Если вам необходимо зашифровать текст, содержащий важную информацию, какой метод, из одноалфавитных, вы выберете? Обоснуйте свой выбор.
4. Целесообразно ли повторно применять для уже зашифрованного текста: а) метод многоалфавитного шифрования? б) метод Цезаря?
5. Чем отличается "псевдооткрытый" текст (текст, полученный при расшифровке по ложному ключу) от настоящего открытого текста?
6. Как зависит время вскрытия шифра описанным выше способом подбора ключей от длины "вероятного" слова?
7. Зависит ли время вскрытия шифра гаммирования (или таблицы Виженера) от мощности алфавита гаммы?
8. В чем недостатки метода дешифрования с использованием протяжки вероятного слова?
9. Сравните основные характеристики алгоритмов *Rijndael* и ГОСТ 28147-89.
10. Сравните выработку ключевой информации в алгоритмах *Rijndael* и ГОСТ 28147-89.
11. Сравните основные характеристики алгоритмов *Rijndael* и *DES*.
12. Опишите структуру сети Фейстеля.
13. Сравните алгоритмы *Rijndael* и ГОСТ 28147-89 по показателям диффузии.
14. Сравните алгоритмы *Rijndael* и ГОСТ 28147-89 по показателям стойкости.

#### **Лабораторные работы для текущего контроля (фрагмент)**

##### **Задание**

1. Для одноалфавитного метода с фиксированным смещением определить установленное в программе смещение.

Для этого:

- просмотреть предварительно созданный с помощью редактора свой текстовый файл;
- выполнить для этого файла шифрование;
- просмотреть в редакторе зашифрованный файл;
- просмотреть гистограммы исходного и зашифрованного текстов,
- описать гистограммы (в чем похожи, чем отличаются) и определить, с каким смещением было выполнено шифрование;
- расшифровать зашифрованный текст:



- 1) с помощью программы, после чего проверить в редакторе правильность расшифрования;
- 2) вручную с помощью гистограмм; описать и объяснить процесс дешифрования.

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов, описываются полученные гистограммы, указывается найденное смещение, описывается процесс дешифрования.

Преподавателю предоставляется отчет о проделанной работе и все использованные и созданные файлы.

2. Для одноалфавитного метода с задаваемым смещением (шифр Цезаря):
  - для своего исходного текста выполнить шифрование с произвольным смещением;
  - просмотреть и описать гистограммы исходного и зашифрованного текстов, определить смещение для нескольких символов;
  - расшифровать текст с помощью программы;
  - имеется зашифрованный шифром Цезаря текст; дешифровать его с помощью программы методом подбора смещения; указать, с каким смещением был зашифрован файл.

3. Для метода перестановки символов дешифровать зашифрованный файл.

Для этого необходимо определить закон перестановки символов открытого текста. Создайте небольшой файл длиной в несколько слов с известным вам текстом, зашифруйте его, просмотрите гистограммы (опишите их; ответьте, можно ли извлечь из них полезную для дешифровки информацию). Сравните (с помощью редактора) ваш исходный и зашифрованный тексты и определите закон перестановки символов.

Дешифруйте файл:

- 1) вручную (объясните ваши действия);
- 2) с помощью программы.

4. Для инверсного кодирования (по дополнению до 255):
  - для своего произвольного файла выполните шифрование;
  - просмотрите гистограммы исходного и зашифрованного текстов, опишите гистограммы и определите смещение для нескольких символов;
  - дешифруйте зашифрованный текст, проверьте в редакторе правильность дешифрования.

5. Для многоалфавитного шифрования с фиксированным ключом определите, сколько одноалфавитных методов и с каким смещением используется в программе.

Для этого нужно создать свой файл, состоящий из строки одинаковых символов, выполнить для него шифрование и по гистограмме определить способ шифрования и набор смещений.

6. Для многоалфавитного шифрования с ключом фиксированной длины:
  - для файла, состоящего из строки одинаковых символов выполнить шифрование и определить по гистограмме, какое смещение получает каждый символ;
  - для файла произвольного текста произвести шифрование и расшифрование;
  - просмотреть и описать гистограммы исходного и зашифрованного текстов; ответить, какую информацию можно получить из гистограмм.

8. Для многоалфавитного шифрования с произвольным паролем задание полностью аналогично п.6.

### **Тестовые задания для текущего контроля (фрагмент)**

1. Согласно закону "Об информации, информатизации и защите информации", риск, связанный с использованием информации, полученной из несертифицированного источника, лежит на:
  - а) потребителе информации
  - б) владельце этой системы
  - в) собственнике документов

2. Действие Закона "О лицензировании отдельных видов деятельности" не распространяется на:
  - а) предоставление услуг в области шифрования информации
  - б) деятельность по технической защите конфиденциальной информации
  - в) образовательную деятельность в области защиты информации
3. Согласно Закону "О лицензировании отдельных видов деятельности", лицензия - это:
  - а) документ, гарантирующий безопасность программного продукта
  - б) специальное разрешение на осуществление конкретного вида деятельности
  - в) удостоверение, подтверждающее высокое качество изделия
4. Уровень безопасности С, согласно "Оранжевой книге", характеризуется:
  - а) верифицируемой безопасностью
  - б) произвольным управлением доступом
  - в) принудительным управлением доступом
5. Уголовный кодекс РФ не предусматривает наказания за:
  - а) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети
  - б) создание, использование и распространение вредоносных программ
  - в) ведение личной корреспонденции на производственной технической базе
6. Согласно закону "Об информации, информатизации и защите информации", персональные данные - это:
  - а) данные, находящиеся в чьей-либо персональной собственности
  - б) сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие
  - в) идентифицировать его личность
  - г) данные, хранящиеся в персональном компьютере
7. В число возможных стратегий нейтрализации рисков входят:
  - а) переадресация риска
  - б) уменьшение риска
  - в) афиширование риска
  - г) декомпозиция риска
8. Первый шаг в анализе угроз - это:
  - а) ликвидация угроз
  - б) идентификация угроз
  - в) аутентификация угроз
9. После идентификации угрозы необходимо оценить:
  - а) вероятность её осуществления
  - б) ущерб от её осуществления
  - в) частоту её осуществления
10. Политика безопасности строится на основе:
  - а) анализа рисков
  - б) общих представлений об ИС организации
  - в) изучения политик родственных организаций
11. В число целей политики безопасности верхнего уровня входят:
  - а) выбор методов аутентификации пользователей
  - б) формулировка целей, которые преследует организация в области ИБ
  - в) обеспечение конфиденциальности почтовых сообщений
  - г) формулировка административных решений по важнейшим аспектам реализации программы безопасности
  - д) обеспечение базы для соблюдения законов и правил
12. В число этапов жизненного цикла информационного сервиса входят:
  - а) выведение из эксплуатации
  - б) закупка
  - в) продажа
13. Главная цель мер, предпринимаемых на административном уровне:

- а) сформировать программу безопасности и обеспечить её выполнение
  - б) выполнить положения действующего законодательства
  - в) отчитаться перед вышестоящими инстанциями
14. В число принципов физической защиты входят:
- а) минимизация защитных средств
  - б) беспощадный отпор
  - в) непрерывность защиты в пространстве и времени
15. В число принципов управления персоналом входят:
- а) инкапсуляция наследования
  - б) минимизация привилегий
  - в) минимизация зарплаты
  - г) "разделяй и властвуй"
  - д) разделение обязанностей

#### 7.4. Соответствие шкалы оценок и уровней сформированности компетенций

По каждой компетенции в зависимости от уровня освоения преподаватель выставляет следующие оценки: «зачтено», «не зачтено». Итоговая оценка по промежуточной аттестации определяется как средне-арифметическая по оценкам компетенций, основываясь на правилах математического округления.

Соответствие шкалы оценок и уровней сформированных компетенций

| Уровень сформированности компетенций | Оценка                         | Пояснение   |
|--------------------------------------|--------------------------------|---|
| Высокий                              | Отлично/зачтено                | Теоретическое содержание дисциплины освоено полностью, все поставленные в ней цели и задачи достигнуты, все предусмотренные программой обучения учебные задания выполнены без замечаний. Компетенции сформирована на высоком уровне.  |
| Базовый                              | Хорошо/зачтено                 | Теоретическое содержание дисциплины освоено полностью, все поставленные в ней цели и задачи достигнуты, все предусмотренные программой обучения учебные задания выполнены с отдельными незначительными замечаниями. Компетенции сформированы на базовом уровне.   |
| Пороговый                            | Удовлетворительно/зачтено      | Теоретическое содержание дисциплины освоено частично, предусмотренные программой обучения учебные задания выполнены с замечаниями. Компетенции сформированы на пороговом уровне.  |
| Низкий                               | Неудовлетворительно/не зачтено | Теоретическое содержание дисциплины не освоено, компетенции не сформирована, большинство предусмотренных программой обучения учебных заданий либо не выполнены, либо содержат грубые ошибки; дополнительная самостоятельная работа над материалом не привела к какому-либо значительному повышению качества выполнения учебных заданий. |

## 8. Методические указания для самостоятельной работы обучающихся

Самостоятельная работа – планируемая учебная, учебно-исследовательская, научно-исследовательская работа магистрантов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосред-

ственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль в контроле за работой студентов и магистрантов).

Самостоятельная работа студентов и магистрантов в вузе является важным видом учебной и научной деятельности. Самостоятельная работа играет значительную роль в рейтинговой технологии обучения. Государственным стандартом предусматривается, как правило, 50% часов из общей трудоемкости дисциплины на самостоятельную работу студентов и магистрантов. В связи с этим, обучение в вузе включает в себя две, практически одинаковые по объему и взаимовлиянию части – процесса обучения и процесса самообучения. Поэтому самостоятельная работа должна стать эффективной и целенаправленной работой студентов и магистрантов.

*Формы самостоятельной работы* магистрантов разнообразны. Они включают в себя:

- изучение и систематизацию официальных государственных документов: законов, постановлений, указов, нормативно-инструкционных и справочных материалов с использованием информационно-поисковых систем «Консультант Плюс», «Гарант», глобальной сети «Интернет»;
- изучение учебной, научной и методической литературы, материалов периодических изданий с привлечением электронных средств официальной, статистической, периодической и научной информации;
- написание рефератов по теме дисциплины;
- создание презентаций, докладов по выполняемому проекту;
- участие в работе конференций, комплексных научных исследованиях;
- Написание научных статей.

В процессе изучения дисциплины «Устойчивость и безопасность функционирования информационных систем» магистрантами направления 09.04.03 *основными видами самостоятельной работы* являются:

- подготовка к аудиторным занятиям (лекциям и практическим занятиям) и выполнение соответствующих заданий;
- самостоятельная работа над отдельными темами учебной дисциплины в соответствии с учебно-тематическим планом;
- написание рефератов;
- подготовка докладов и презентаций;
- написание научных статей;
- выполнение тестовых заданий;
- подготовка к зачету с оценкой.

*Подготовка рефератов и докладов* по выбранной тематике предполагает подбор необходимого материала и его анализ, определение его актуальности и достаточности, формирование плана доклада или структуры реферата, таким образом, чтобы тема была полностью раскрыта. Изложение материала должно быть связным, последовательным, доказательным. Способ изложения материала для выступления должен носить конспективный или тезисный характер. Подготовленная в PowerPoint презентация должна иллюстрировать доклад и быть удобной для восприятия.

Если Вас заинтересовала какая-то другая тема, даже если её вообще нет в перечне тем, то после обсуждения с преподавателем (имеет ли она отношение к дисциплине и её содержательный объем) её можно выбрать. Поскольку понятие ИС весьма общее, при раскрытии те-

мы реферата можно ограничиться отдельным, определенным видом ИС. Выбранный Вами вид ИС необходимо согласовать с преподавателем.

Необходимо учитывать, что практические занятия для магистрантов организованы в виде последовательности прохождения этапов подготовки реферата (обзора) современного состояния дел в одной из проблемных областей, связанных с тематикой «Устойчивости и безопасности функционирования информационных систем». Занятия проводятся в индивидуальном режиме, то есть каждый магистрант получает свою, индивидуальную тему и поэтапно самостоятельно готовит реферат, доклад и презентацию. Цель – приобретение минимальных навыков **самостоятельной научной работы**.

Итоговый текст реферата должен быть объемом не больше 20 страниц, но это не догма. По содержанию – должны быть рассмотрены **различные** подходы к проблематике темы. Дано краткое, но исчерпывающее описание каждого подхода, проведен сравнительный их анализ – то есть, что в подходах общее, а чем отличаются. Далее изложен собственный взгляд на проблематику. Как минимум – Вы присоединяетесь к одному из рассмотренных подходов и мотивируете: почему считаете его лучшим. Одобряется попытка обобщения нескольких подходов.

Первый этап (тема первых двух практических занятий) – составление, обсуждение с преподавателем и доработка до приемлемого уровня аннотированного списка источников, по содержанию которых далее будет, также поэтапно формироваться текст.

Аннотированный список источников отличается от списка источников тем, что после оформленной в соответствии со стандартами ссылки на источник приводится краткая аннотация по его содержанию. Обычно один, два абзаца. Желательно, что бы дополнительно Вы написали: почему он был Вами включен в список. Список должен содержать не менее 15 ссылок (по опыту по предлагаемым темам 20 – 25).

## **9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине**

Для успешного овладения дисциплиной используются следующие информационные технологии обучения:

– операционная система Windows 7, License 49013351 УГЛТУ Russia 2011-09-06, OPEN 68975925ZZE1309. Срок: бессрочно;

- операционная система AstraLinuxSpecialEdition. Договор №Pr000013979/0385/22-ЕП-223-06 от 01.07.2022. Срок: бессрочно;

– пакет прикладных программ Office Professional Plus 2010, License 49013351 УГЛТУ Russia 2011-09-06, OPEN 68975925ZZE1309. Срок: бессрочно;

– пакет прикладных программ Р7-Офис.Профессиональный. Договор №Pr000013979/0385/22-ЕП-223-06 от 01.07.2022. Срок: бессрочно;

– антивирусная программа KasperskyEndpointSecurity для бизнеса-Стандартный RussianEdition. 250-499 Node 1 year Educational Renewal License. Договор №0423/3Кот 30.08.2022. Срокс 09.10.2022 г. по 09.10.2023 г.;

– операционная система WindowsServer. Контракт на услуги по предоставлению лицензий на право использовать компьютерное обеспечение № 067/ЭА от 07.12.2020 года. Срок бессрочно;

– система видеоконференцсвязи Mirapolis. Договор №57/03/23-К/0148/23-ЕП-223-03 от 13.03.2023. Срок: с 13.03.2023 по 13.03.2024;

– система видеоконференцсвязи Пруффми. Договор № 2576620 -1/ 0147 / 23-ЕП-223-03 от 15.03.2023. Срок: с 15.03.2023 по 15.03.2024;

– система управления обучением LMS Moodle – программное обеспечение с открытым кодом, распространяется по лицензии GNU PublicLicense (rus);

- браузер Yandex (<https://yandex.ru/promo/browser/>) – программное обеспечение распространяется по простой (неисключительной) лицензии;
- платформа 1С: Предприятие 8. Договор №0164/ЗК от 31.05.2021 г. Срок действия: бессрочно;
- система управления данными Microsoft SQL Server. Контракт на услуги по предоставлению лицензий на право использовать компьютерное обеспечение № 067/ЭА от 07.12.2020 года. Срок бессрочно;
- интегрированная среда для разработки VisualStudio. Контракт на услуги по предоставлению лицензий на право использовать компьютерное обеспечение № 067/ЭА от 07.12.2020 года. Срок бессрочно;
- система управления реляционными базами данных MySQL (<https://www.mysql.com/>) – программное обеспечение с открытым кодом, распространяется по лицензии GNU GPL 2 и проприетарной лицензии;
- Apache HTTP-сервер (<http://httpd.apache.org>) – программное обеспечение с открытым кодом, распространяется по лицензии ApacheLicense;
- скриптовый язык общего назначения PHP ([php.net](http://php.net)) – программное обеспечение с открытым исходным кодом, распространяется по лицензии PHP License;
- система управления базами данных PostgreSQL (<https://www.postgresql.org/download/windows/>) – программное обеспечение с открытым кодом OpenSource, распространяется по лицензии PostgreSQLLicense;
- платформа Eucalyptus (<https://www.eucalyptus.cloud/>) - программное обеспечение с открытым исходным кодом, распространяется по стандартной общественной лицензии GNU (GPL);
- система бизнес-моделирования UMLetino (<http://www.umlet.com/umletino/umletino.html>) – свободно распространяемое программное обеспечение OpenSource, распространяется по лицензии GNU (GPL);
- приложение ApacheJMeter ([jmeter.apache.org](http://jmeter.apache.org)) – программное обеспечение с открытым исходным кодом, применяется согласно лицензии APACHE;
- программное обеспечение для автоматизации тестирования настольных, мобильных и веб-приложений Sahi – программное обеспечение с открытым исходным кодом OpenSource, выпущен под лицензией ApacheLicense 2.0;
- интерпретатор языка программирования Python ([www.python.org](http://www.python.org)) – программное обеспечение с открытым исходным кодом, распространяется в соответствии с Лицензионным соглашением PSF и лицензией BSD;
- пакет прикладных математических программ Scilab 6.1.0 (<https://www.scilab.org/download/6.1.0>) – свободно распространяемое программное обеспечение, распространяется по лицензии GNU GeneralPublicLicense (GPL) v2.0;
- программа для эмуляции работы сети NetEmul (<http://netemul.sourceforge.net/ruindex.html>) – свободно распространяемое программное обеспечение, распространяется по лицензии GPL.

## **10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Реализация учебного процесса осуществляется в специальных учебных аудиториях университета для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Все аудитории укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. При необходимости обучающимся предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации.

Самостоятельная работа обучающихся выполняется в специализированной аудитории, которая оборудована учебной мебелью, компьютерной техникой с возможностью

подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УГЛТУ.

Есть помещение для хранения и профилактического обслуживания учебного оборудования.

### Требования к аудиториям

| Наименование специальных помещений и помещений для самостоятельной работы                                      | Оснащенность специальных помещений и помещений для самостоятельной работы   |
|--|---|
| Помещение для лекционных занятий, групповых и индивидуальных консультаций, текущей и промежуточной аттестации. | Переносные:<br>- демонстрационное мультимедийное оборудование (ноутбук, проектор);<br>- комплект электронных учебно-наглядных материалов (презентаций) на флеш-носителях, обеспечивающих тематические иллюстрации. Столы и стулья. Экран.               |
| Помещение для лабораторных занятий   | Компьютерные классы:<br>оборудование кабинета: компьютеры, доска аудиторная (интерактивная); демонстрационное мультимедийное оборудование: проектор; рабочее место преподавателя: стол, стул.   |
| Помещения для самостоятельной работы   | Столы компьютерные, стулья. Персональные компьютеры. Выход в Интернет, электронную образовательную среду университета.  |
| Помещение для хранения и профилактического обслуживания оборудования   | Переносное демонстрационное оборудование (мультимедийные проекторы, экраны, ноутбуки). Расходные материалы для ремонта и обслуживания техники. Шкаф (стеллаж) для хранения экспонатов, таблиц, раздаточного материала. Места для хранения оборудования. |