МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
**Федеральное государственное бюджетное образовательное учреждение высшего образования**
**«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»**
**(ФГБОУ ВО «КГЭУ»)**



УТВЕРЖДАЮ
Директор Института цифровых технологий и экономики
_____ Э.И. Беляев
«30» 05 2023 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

# Б1.О.13.05 Информационная безопасность

| | |
|---|---|
| Направление подготовки | 01.03.04 Прикладная математика |
| Направленность (профиль) подготовки | Математическое и программное обеспечение систем искусственного интеллекта |
| Квалификация | Бакалавр |

г. Казань, 2023

Программу разработал(и):

| Наименование кафедры | Должность, уч.степень, уч.звание | ФИО разработчика |
|---|---|---|
| ИТИС | доцент, к.т.н. | Исмагилов И.Р. |

| Согласование | Наименование подразделения | Дата | № протокола | Подпись |
|---|---|---|---|---|
| Одобрена | ИТИС | 27.04.23 | 3 | Зав.каф., д.п.н., доц. Торкунова Ю. В. |
| Согласовано | ЦСМ | 19.05.23 | 5 | Зав.каф., к.ф.-м.н., доц. Смирнов Ю. Н. |
| Согласована | Учебно-методический совет ИЦТЭ | 30.05.23 | 7 | Директор, к.т.н., доц. Беляев Э.И. |
| Одобрена | Ученый совет ИЦТЭ | 30.05.23 | 9 | Директор, к.т.н., доц. Беляев Э.И. |

## 1. Цель, задачи и планируемые результаты обучения по дисциплине

(*Цель и задачи освоения дисциплины, соответствующие цели ОП*)

Целью освоения дисциплины «Информационная безопасность» является получение базовых теоретических представлений о современных методах и средствах защиты информации и практических навыков использования этих средств при реализации программных и аппаратных средств информационных систем масштаба предприятия

Задачами дисциплины являются:

1. формирование знаний

- терминологии в области информационной безопасности и защиты информации
- основных нормативных и правовых актов, регламентирующих сферу информационной безопасности и защиты информации
- принципов организации защиты информации на предприятиях;
- мер и средств защиты информации

2. формирование умений

- выявлять основные виды угроз и уязвимостей безопасности информации;
- разрабатывать нормативно-техническую документацию с учетом требований нормативных и правовых актов в области информационной безопасности и защиты информации
- криптографические методы обеспечения целостности и конфиденциальности информации

3. формирование владения:

- навыками применения программно-аппаратных средств для обеспечения информационной безопасности
- навыками программной реализации криптографических алгоритмов

Компетенции и индикаторы, формируемые у обучающихся:

| Код и наименование компетенции | Код и наименование индикатора |
|---|---|
| ОПК-3 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности; | ОПК-3.2 Способен применять современные информационные технологии при решении задач профессиональной деятельности |

## 2. Место дисциплины в структуре ОП

Предшествующие дисциплины (модули), практики, НИР, др.: Высшая математика, Физика, Информационные технологии, Алгоритмизация и программирование

Последующие дисциплины (модули), практики, НИР, др. Выполнение и защита выпускной квалификационной работы

## 3. Структура и содержание дисциплины

### 3.1. Структура дисциплины

Для очной формы обучения

| Вид учебной работы | Всего ЗЕ | Всего часов | Семестр(ы) |
|---|---|---|---|
| | | | 3 |
| ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ | 3 | 108 | 108 |
| КОНТАКТНАЯ РАБОТА* | - | 72 | 72 |
| АУДИТОРНАЯ РАБОТА | - | 68 | 68 |
| Лекции | - | 34 | 34 |
| Практические (семинарские) занятия | - | 0 | 0 |
| Лабораторные работы | - | 34 | 34 |
| САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ | - | 40 | 40 |
| Проработка учебного материала | - | 4 | 4 |
| Курсовой проект | - | 0 | 0 |
| Курсовая работа | - | 0 | 0 |
| Подготовка к промежуточной аттестации | - | 0 | 0 |
| Промежуточная аттестация: | | | 3 |
| | | | - |

Для заочной формы обучения

| Вид учебной работы | Всего ЗЕ | Всего часов | Семестр(ы) |
|---|---|---|---|
| | | | 3 |
| ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ | 3 | 108 | 108 |
| КОНТАКТНАЯ РАБОТА* | - | 25 | 25 |
| АУДИТОРНАЯ РАБОТА | - | 18 | 18 |
| Лекции | - | 10 | 10 |
| Практические (семинарские) занятия | - | 0 | 0 |
| Лабораторные работы | - | 8 | 8 |
| САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ | - | 86 | 86 |
| Проработка учебного материала | - | 7 | 7 |
| Контрольная работа | | 18 | 18 |
| Курсовой проект | - | 0 | 0 |
| Курсовая работа | - | 0 | 0 |
| Подготовка к промежуточной аттестации | - | 0 | 0 |
| Промежуточная аттестация: | | | 3 |
| | | | - |

### 3.2. Содержание дисциплины, структурированное по разделам и видам занятий

| Разделы дисциплины | Всего часов | Распределение трудоемкости по видам учебной работы | | | | Формы и вид контроля | Индексы индикаторов формируемых компетенций |
|---|---|---|---|---|---|---|---|
| | | лекции | лаб. раб. | пр. зан. | сам. раб. | | |
| Раздел 1 | 14 | 4 | 4 | 0 | 6 | ТК1 | ОПК-3.З |
| Раздел 2 | 8 | 2 | 4 | 0 | 4 | ТК1 | ОПК-3.З, ОПК-3.У |
| Раздел 3 | 18 | 4 | 8 | 0 | 6 | ТК2 | ОПК-3.У, ОПК-3.В |
| Раздел 4 | 14 | 4 | 4 | 0 | 6 | ТК3 | ОПК-3.З, ОПК-3.У |
| Раздел 5 | 14 | 4 | 4 | 0 | 6 | ТК3 | ОПК-3.З, ОПК-3.У |
| Раздел 6 | 12 | 4 | 2 | 0 | 6 | ТК3 | ОПК-3.З |
| Раздел 7 | 18 | 4 | 8 | 0 | 6 | ТК4 | ОПК-3.З, ОПК-3.У |
| Зачет | 0 | 0 | 0 | 0 | 0 | **ОМ** | ОПК-3.З, ОПК-3.У |
| **Итого за 3 семестр** | **108** | **34** | **34** | **0** | **40** | | |
| **ИТОГО** | **108** | **34** | **34** | **0** | **40** | | |

### 3.3. Содержание дисциплины

Раздел 1. Основные понятия и нормативно-правовая база информационной безопасности

Тема 1.1. Основные понятия информационной безопасности

Тема 1.2. Государственная политика в области информационной безопасности

Тема 1.3. Классификация информации, доступ к которой ограничен федеральными законами РФ

Тема 1.4. Модель угроз безопасности информации предприятия

Раздел 2. Управление информационной безопасностью

Тема 2.1. Международные и российские стандарты в сфере информационной безопасности

Тема 2.2. Политика информационной безопасности

Тема 2.3. Менеджмент рисков информационной безопасности предприятия

Раздел 3. Меры и средства защиты информации. Криптографические средства защиты информации (КСЗИ)

Тема 3.1. Симметричные криптосистемы шифрования. Стандарты шифрования DES, 3DES, AES, ГОСТ 28147-89.

Тема 3.2. Стеганографические методы защиты информации

Тема 3.3 Асимметричные криптосистемы шифрования

Тема 3.4 Защита информации в электронных документах путем шифрования и формирования электронной подписи

Тема 3.5 Управление криптоключами. Инфраструктура открытых ключей (PKI)

Раздел 4. Идентификация, аутентификация и управление доступом

Тема 4.1 Технологии аутентификации

Тема 4.2 Криптографические протоколы аутентификации. Биометрическая аутентификация
Тема 4.3 Модели разграничения доступа

Раздел 5. Обеспечение безопасности информации в операционных системах
Тема 5.1 Обеспечение безопасности информации в операционных системах семейства Windows/Linux
Тема 5.2 Автоматизированное обнаружение уязвимостей программного обеспечения на рабочих станциях под управлением операционных систем семейства Microsoft Windows
Тема 5.3 Локальные и групповые политики безопасности ОС Microsoft Windows

Раздел 6. Средства антивирусной защиты (САВЗ)
Тема 6.1 Классификация вредоносных программ
Тема 6.2 Средства антивирусной защиты информации
Тема 6.3 Сравнительный анализ средств антивирусной защиты информации с использованием результатов независимых тестов

Раздел 7. Обеспечение безопасности информации в компьютерных сетях
Тема 7.1 Классификация угроз безопасности информации и атак в компьютерных сетях согласно уровням модели OSI
Тема 7.2 Технология виртуальных локальных сетей (VLAN)
Тема 7.3 Технологии межсетевого экранирования
Тема 7.4 Технологии виртуальных частных сетей (VPN)
Тема 7.5 Изучение средств инструментального анализа защищенности ИТ-инфраструктуры

**3.4. Тематический план практических занятий**

Данный вид работы не предусмотрен учебным планом

**3.5. Тематический план лабораторных работ**

1. Разработка модели угроз безопасности информации предприятия
2. Анализ рисков информационной безопасности предприятия
3. Моноалфавитные и полиалфавитные шифры. Частотный криптоанализ
4. Программная реализация классических алгоритмов шифрования и их криптоанализа
5. Защита информации в электронных документах путем шифрования и формирования электронной подписи
6. Парольная аутентификация.
7. Администрирование пользователей и правил разграничения доступа в ОС Astra Linux.pdf
8. Изучение технологий виртуальных локальных сетей (VLAN) с помощью программы моделирования сетей Cisco Packet Tracer
9. Изучение технологий межсетевого экранирования с помощью программы моделирования сетей Cisco Packet Tracer

**3.6. Курсовой проект /курсовая работа**

Данный вид работы не предусмотрен учебным планом

## 4. Оценивание результатов обучения

Оценивание результатов обучения по дисциплине осуществляется в рамках текущего контроля и промежуточной аттестации, проводимых по балльно-рейтинговой системе (БРС).

Шкала оценки результатов обучения по дисциплине:

| | | | | | | |
|---|---|---|---|---|---|---|
| Код компе-тенции | Код индикатора компетенции | Заплани-рованные результаты обучения по дисциплине | Уровень сформированности индикатора компетенции | | | |
| | | | Высокий | Средний | Ниже среднего | Низкий |
| | | | от 85 до 100 | от 70 до 84 | от 55 до 69 | от 0 до 54 |
| | | | Шкала оценивания | | | |
| | | | отлично | хорошо | удовлет-ворительно | неудов-летвори-тельно |
| | | | зачтено | | | не зачтено |
| | ОПК-3.2 | знать: | | | | |
| | | основные виды угроз безопасности информации, уязвимостей информационных систем, а также меры и средства противодействия атакам на информационные ресурсы при проектировании, разработке и внедрении программного обеспечения информационных систем | Уровень знаний в объеме, соответствующем программе подготовки, без ошибок | Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых ошибок | Минимально допустимый уровень знаний, имеет место много негрубых ошибок | Уровень знаний ниже минимальных требований, имеют место грубые ошибки |
| | | уметь: | | | | |
| | | разрабатывать проектно-техническую документацию для информационных систем с учетом требований | Продемонстрированы все основные умения, решены все основные | Продемонстрированы все основные умения, решены все основные | Продемонстрированы основные умения, решены типовые задачи с негрубым | При решении стандартных задач не продемонстрированы основные |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | текущего законодательства, нормативно-правовых актов, стандартов и ведущих практик в области информационной безопасности | задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме | задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами | и ошибками, выполнены все задания, но не в полном объеме | умения, имеют место грубые ошибки |
| | | владеть: | | | | |
| | | навыками применения программно-аппаратных средств для анализа защищенности информационных систем для выработки мер противодействия известным угрозам безопасности информации | Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов | Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами | Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами | При решении стандартных задач не продемонстрированы базовые навыки, имеют место грубые ошибки |

Оценочные материалы для проведения текущего контроля и промежуточной аттестации приведены в Приложении к рабочей программе дисциплины.

Полный комплект заданий и материалов, необходимых для оценивания результатов обучения по дисциплине, хранится на кафедре разработчика.

## 5. Учебно-методическое и информационное обеспечение дисциплины

### 5.1. Учебно-методическое обеспечение

Основная литература

1. Литвиненко, В. И., Основы информационной безопасности : учебное пособие / В. И. Литвиненко, Е. С. Козлов. — Москва : КноРус, 2022. — 199 с. — ISBN 978-5-406-09438-9. — URL: https://book.ru/book/943111. — Текст : электронный.
2. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. —

ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206279.
3. Мельников, В. П., Информационная безопасность : учебник / В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. — Москва : КноРус, 2023. — 371 с. — ISBN 978-5-406-11960-0. — URL: https://book.ru/book/950148. — Текст: электронный.
4. Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/293009.

Дополнительная литература

1. Николаев, Н. С., Управление информационной безопасностью : учебник / Н. С. Николаев. — Москва : КноРус, 2021. — 188 с. — ISBN 978-5-406-07325-4. — URL: https://book.ru/book/939841. — Текст : электронный.
2. Ванюшина, А. В. Основы информационной безопасности : учебно-методическое пособие / А. В. Ванюшина, С. Ю. Рыбаков. — Москва : МТУСИ, 2022. — 22 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/333701. — Режим доступа: для авториз. пользователей.
3. Баранова, Е. К., Криптографические методы защиты информации. Лабораторный практикум + еПриложение : учебное пособие / Е. К. Баранова, А. В. Бабаш. — Москва : КноРус, 2022. — 205 с. — ISBN 978-5-406-08831-9. — URL: https://book.ru/book/941742. — Текст : электронный.
4. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401. ***(добавлено)***

### 5.2. Информационное обеспечение

5.2.1 Электронные и интернет-ресурсы

| № п/п | Наименование электронных и интернет-ресурсов | Ссылка |
|---|---|---|
| 1 | Справочно-правовая система "Консультант | http://www.consultant.ru/ |
| 2 | Справочно-правовая система "Гарант" | http://www.garant.ru/ |
| 3 | Банк данных угроз безопасности информации | https://bdu.fstec.ru/ |
| 4 | Методика оценки угроз безопасности информации | https://fstec.ru/files/495/---5--2021-/891/---5--2021-.pdf |
| 5 | ISO27000 - Искусство управления информационной безопасностью | http://www.iso27000.ru/standarty |

| | | |
|---|---|---|
| 6 | Учебный курс на портале НОУ "ИНТУИТ" - Стандарты информационной безопасности | https://www.intuit.ru/studies/courses/30/30/info |
| 7 | Учебный курс на портале НОУ "ИНТУИТ" - Информационная безопасность. Технологии | https://www.intuit.ru/studies/professional_retraining/952/courses/419 |
| 8 | Учебный курс на портале НОУ "ИНТУИТ" - Информационная безопасность. Технологии | https://www.intuit.ru/studies/professional_retraining/952/courses/387 /info |
| 9 | Anti-Malware Testing Standards Organization | https://www.amtso.org/ |
| 10 | AV-TEST - The Independent IT-Security Institute | https://www.av-test.org/en/ |
| 11 | AV-Comparatives - Independent Tests of Anti-Virus Software | https://www.av-comparatives.org/ |
| 12 | Wireshark — программа-анализатор трафика для компьютерных сетей Ethernet | https://www.wireshark.org/ |
| 13 | Справочное руководство Nmap на русском языке | https://nmap.org/man/ru/index.htm l |
| 14 | OpenVAS Russia. Русскоязычное сообщество пользователей сканера уязвимостей OpenVAS | https://openvas.ru/ |
| 15 | Cisco Networking Academy | https://www.netacad.com/ |
| 16 | Cisco Networking Academy - маршрутизация и коммутация | http://ccna.mpei.ac.ru/RoutingAndSwitching/ |

5.2.2. Профессиональные базы данных

| № п/п | Наименование профессиональных баз данных | Адрес | Режим доступа |
|---|---|---|---|
| 1 | Российская национальная | http://nlr.ru/ | http://nlr.ru/ |
| 2 | Научная электронная библиотека eLIBRARY.RU | http://elibrary.ru | http://elibrary.ru |

5.2.3. Информационно-справочные системы

| № п/п | Наименование информационно-справочных систем | Адрес | Режим доступа |
|---|---|---|---|
| 1 | ИСС «Кодекс» / «Техэксперт» | http://app.kgeu.local/Home/Ap ps | http://app.kgeu.local/Home/Apps |
| 2 | «Гарант» | http://www.garant.ru/ | http://www.garant.ru/ |
| 3 | «Консультант плюс» | http://www.consultant.ru/ | http://www.consultant.ru/ |

5.2.4. Лицензионное и свободно распространяемое программное обеспечение дисциплины

| № п/п | Наименование программного обеспечения | Способ распространения (лицензионное/свободно) | Реквизиты подтверждающих документов |
|---|---|---|---|
| 1 | Браузер Chrome | Система поиска информации в сети интернет (включая | https://www.google.com /intl/ru/chrome/ |

| | | | |
|---|---|---|---|
| 2 | Браузер Firefox | Свободный веб-браузер | https://www.mozilla.org/ ru/firefox/new/ |
| 3 | OpenOffice | Пакет офисных приложений.Одним из первых стал поддерживать новый открытый формат OpenDocument. Официально поддерживается на платформах Linux | https://www.openoffice. org/ru/download/index.h tml |
| 4 | Adobe Acrobat | Пакет программ | https://get.adobe.com/ru/ reader/ |
| 5 | LMS Moodle | Это современное программное обеспечение | https://download.moodle .org/releases/latest/ |
| 6 | Windows 7 Профессиональная (Pro) | Пользовательская операционная система | №2011.25486 от 28.11.2011 |

## 6. Материально-техническое обеспечение дисциплины

| Наименование вида учебной работы | Наименование учебной аудитории, специализированной лаборатории | Перечень необходимого оборудования и технических средств обучения |
|---|---|---|
| Лекции | Учебная аудитория для проведения занятий лекционного типа | Специализированная учебная мебель, технические средства обучения, служащие для представления учебной информации большой аудитории (мультимедийный проектор, компьютер (ноутбук), экран), демонстрационное оборудование, учебно-наглядные пособия |
| Лабораторные работы | Учебная лаборатория программной инженерии, ауд. В-608 | Специализированное лабораторное оборудование по профилю лаборатории программной инженерии, специализированная учебная мебель на 50 посадочных мест, 24 компьютера с возможностью выхода в Интернет и обеспечением доступа в ЭИОС, технические средства обучения (мультимедийный проектор, мультимедийная доска, моноблок), необходимое лицензионное программное обеспечение |
| | Компьютерный класс, ауд. В-610 | Специализированная учебная мебель на 42 посадочных места, 17 компьютеров с возможностью выхода в Интернет и обеспечением доступа в ЭИОС, технические средства обучения (мультимедийный проектор, экран для проектора, моноблок), необходимое лицензионное программное обеспечение |
| | Учебная лаборатория информационной безопасности, | Специализированное лабораторное оборудование по профилю лаборатории информационной безопасности, |

| | | |
|---|---|---|
| | ауд. В-615 | специализированная учебная мебель на 35 посадочных мест, 15 компьютеров с возможностью выхода в Интернет и обеспечением доступа в ЭИОС, технические средства обучения (мультимедийный проектор, мультимедийная доска, моноблок), необходимое лицензионное программное обеспечение |
| | Компьютерный класс, ауд. В-617 | Специализированная учебная мебель на 24 посадочных места, 21 компьютер с возможностью выхода в Интернет и обеспечением доступа в ЭИОС, необходимое лицензионное программное обеспечение |
| | Компьютерный класс, ауд. В-619 | Специализированная учебная мебель на 26 посадочных мест, 21 компьютер с возможностью выхода в Интернет и обеспечением доступа в ЭИОС, необходимое лицензионное программное обеспечение |
| | Компьютерный класс, ауд. В-621 | Специализированная учебная мебель на 35 посадочных мест, 13 компьютеров с возможностью выхода в Интернет и обеспечением доступа в ЭИОС, технические средства обучения (мультимедийный проектор, экран для проектора, моноблок), необходимое лицензионное программное обеспечение |
| | Учебная лаборатория реинжиниринга и управления бизнес-процессами, ауд. В-623 | Специализированное лабораторное оборудование по профилю лаборатории реинжиниринга и управления бизнес-процессами, специализированная учебная мебель на 34 посадочных места, 13 компьютеров с возможностью выхода в Интернет и обеспечением доступа в ЭИОС, технические средства обучения (мультимедийный проектор, мультимедийная доска, моноблок), необходимое лицензионное программное обеспечение |
| | Компьютерный класс, В-600 | Специализированная учебная мебель на 30 посадочных мест, 30 компьютеров, компьютеров с возможностью выхода в Интернет и обеспечением доступа в ЭИОС, технические средства обучения (мультимедийный проектор, ноутбук, экран), видеокамеры, необходимое лицензионное программное обеспечение |
| Самостоятельная работа | Компьютерный класс с возможностью выхода в Интернет и обеспечением | Специализированная учебная мебель на 30 посадочных мест, 30 компьютеров, технические средства обучения (мультиме- |

| | | |
|---|---|---|
| | доступа в ЭИОС<br>В-600 | дийный проектор, компьютер (ноутбук), экран), видеокамеры, программное обеспечение |
| | Читальный зал библиотеки | Специализированная мебель, компьютерная техника с возможностью выхода в Интернет и обеспечением доступа в ЭИОС, экран, мультимедийный проектор, программное обеспечение |

## 7. Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья и инвалидов

Лица с ограниченными возможностями здоровья (ОВЗ) и инвалиды имеют возможность беспрепятственно перемещаться из одного учебно-лабораторного корпуса в другой, подняться на все этажи учебно-лабораторных корпусов, заниматься в учебных и иных помещениях с учетом особенностей психофизического развития и состояния здоровья.

Для обучения лиц с ОВЗ и инвалидов, имеющих нарушения опорно-двигательного аппарата, обеспечены условия беспрепятственного доступа во все учебные помещения. Информация о специальных условиях, созданных для обучающихся с ОВЗ и инвалидов, размещена на сайте университета www//kgeu.ru. Имеется возможность оказания технической помощи ассистентом, а также услуг сурдопереводчиков и тифлосурдопереводчиков.

Для адаптации к восприятию лицами с ОВЗ и инвалидами с нарушенным слухом справочного, учебного материала по дисциплине обеспечиваются следующие условия:

- для лучшей ориентации в аудитории, применяются сигналы оповещения о начале и конце занятия (слово «звонок» пишется на доске);
- внимание слабослышащего обучающегося привлекается педагогом жестом (на плечо кладется рука, осуществляется нерезкое похлопывание);
- разговаривая с обучающимся, педагогический работник смотрит на него, говорит ясно, короткими предложениями, обеспечивая возможность чтения по губам.

Компенсация затруднений речевого и интеллектуального развития слабослышащих обучающихся проводится путем:

- использования схем, диаграмм, рисунков, компьютерных презентаций с гиперссылками, комментирующими отдельные компоненты изображения;
- регулярного применения упражнений на графическое выделение существенных признаков предметов и явлений;
- обеспечения возможности для обучающегося получить адресную консультацию по электронной почте по мере необходимости.

Для адаптации к восприятию лицами с ОВЗ и инвалидами с нарушениями зрения справочного, учебного, просветительского материала, предусмотренного образовательной программой по выбранному направлению подготовки, обеспечиваются следующие условия:

- ведется адаптация официального сайта в сети Интернет с учетом особых потребностей инвалидов по зрению, обеспечивается наличие крупношрифтовой справочной информации о расписании учебных занятий;

- педагогический работник, его собеседник (при необходимости), присутствующие на занятии, представляются обучающимся, при этом каждый раз называется тот, к кому педагогический работник обращается;

- действия, жесты, перемещения педагогического работника коротко и ясно комментируются;

- печатная информация предоставляется крупным шрифтом (от 18 пунктов), тотально озвучивается;

- обеспечивается необходимый уровень освещенности помещений;

- предоставляется возможность использовать компьютеры во время занятий и право записи объяснений на диктофон (по желанию обучающихся).

Форма проведения текущей и промежуточной аттестации для обучающихся с ОВЗ и инвалидов определяется педагогическим работником в соответствии с учебным планом. При необходимости обучающемуся с ОВЗ, инвалиду с учетом их индивидуальных психофизических особенностей дается возможность пройти промежуточную аттестацию устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п., либо предоставляется дополнительное время для подготовки ответа.

## 8. Методические рекомендации для преподавателей по организации воспитательной работы с обучающимися.

Методическое обеспечение процесса воспитания обучающихся выступает одним из определяющих факторов высокого качества образования. Преподаватель вуза, демонстрируя высокий профессионализм, эрудицию, четкую гражданскую позицию, самодисциплину, творческий подход в решении профессиональных задач, в ходе образовательного процесса способствует формированию гармоничной личности.

При реализации дисциплины преподаватель может использовать следующие методы воспитательной работы:

- методы формирования сознания личности (беседа, диспут, внушение, инструктаж, контроль, объяснение, пример, самоконтроль, рассказ, совет, убеждение и др.);

- методы организации деятельности и формирования опыта поведения (задание, общественное мнение, педагогическое требование, поручение, приучение, создание воспитывающих ситуаций, тренинг, упражнение, и др.);

- методы мотивации деятельности и поведения (одобрение, поощрение социальной активности, порицание, создание ситуаций успеха, создание ситуаций для эмоционально-нравственных переживаний, соревнование и др.)

При реализации дисциплины преподаватель должен учитывать следующие направления воспитательной деятельности:

*Гражданское и патриотическое воспитание:*

- формирование у обучающихся целостного мировоззрения, российской идентичности, уважения к своей семье, обществу, государству, принятым в семье и

обществе духовно-нравственным и социокультурным ценностям, к национальному, культурному и историческому наследию, формирование стремления к его сохранению и развитию;

- формирование у обучающихся активной гражданской позиции, основанной на традиционных культурных, духовных и нравственных ценностях российского общества, для повышения способности ответственно реализовывать свои конституционные права и обязанности;

- развитие правовой и политической культуры обучающихся, расширение конструктивного участия в принятии решений, затрагивающих их права и интересы, в том числе в различных формах самоорганизации, самоуправления, общественно-значимой деятельности;

- формирование мотивов, нравственных и смысловых установок личности, позволяющих противостоять экстремизму, ксенофобии, дискриминации по социальным, религиозным, расовым, национальным признакам, межэтнической и межконфессиональной нетерпимости, другим негативным социальным явлениям.

*Духовно-нравственное воспитание:*

- воспитание чувства достоинства, чести и честности, совестливости, уважения к родителям, учителям, людям старшего поколения;

- формирование принципов коллективизма и солидарности, духа милосердия и сострадания, привычки заботиться о людях, находящихся в трудной жизненной ситуации;

- формирование солидарности и чувства социальной ответственности по отношению к людям с ограниченными возможностями здоровья, преодоление психологических барьеров по отношению к людям с ограниченными возможностями;

- формирование эмоционально насыщенного и духовно возвышенного отношения к миру, способности и умения передавать другим свой эстетический опыт.

*Культурно-просветительское воспитание:*

- формирование эстетической картины мира;

- формирование уважения к культурным ценностям родного города, края, страны;

- повышение познавательной активности обучающихся.

*Научно-образовательное воспитание:*

- формирование у обучающихся научного мировоззрения;

- формирование умения получать знания;

- формирование навыков анализа и синтеза информации, в том числе в профессиональной области.

**Вносимые изменения и утверждения на новый учебный год**

| № п/п | № раздела внесения изменений | Дата внесения изменений | Содержание изменений | «Согласовано» Зав. каф. реализующей дисциплину | «Согласовано» председатель УМК института (факультета), в состав которого входит |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |

*Приложение к рабочей программе дисциплины*

К Г Э У

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
**Федеральное государственное бюджетное образовательное учреждение высшего образования**
**«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»**
**(ФГБОУ ВО «КГЭУ»)**

# ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
## по дисциплине

Информационная безопасность
*(Наименование дисциплины в соответствии с учебным планом)*

Направление подготовки 01.03.04 Прикладная математика
(*Код и наименование направления подготовки*)

Квалификация Бакалавр
(*Бакалавр / Магистр*)

г. Казань, 2023

Оценочные материалы по дисциплине «Информационная безопасность», предназначенны для оценивания результатов обучения на соответствие индикаторам достижения компетенций.

Оценивание результатов обучения по дисциплине осуществляется в рамках текущего контроля (ТК) и промежуточной аттестации, проводимых по балльно-рейтинговой системе (БРС).

## 1.Технологическая карта

Семестр 3

| Наименование раздела | Формы и вид контроля | Рейтинговые показатели | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | I текущий контроль | Дополнительные баллы к ТК1 | II текущий контроль | Дополнительные баллы к ТК2 | III текущий контроль | Дополнительные баллы к ТК3 | IV текущий контроль | Дополнительные баллы к ТК4 | Итого | Промежуточная аттестация |
| **Раздел 1. «Основные понятия и нормативно-правовая база информационной безопасности»** | **ТК1** | **11** | **0-2** | | | | | | | **11-13** | |
| Тест или письменный опрос | | 2 | | | | | | | | | |
| Защита лабораторной работы | | 4 | | | | | | | | | |
| **Раздел 2. «Управление информационной безопасностью»** | | | | | | | | | | | |
| Тест или письменный опрос | | 1 | | | | | | | | | |
| Защита лабораторной работы | | 4 | | | | | | | | | |
| **Раздел 3. « Меры и средства защиты информации. Криптографические средства** | **ТК2** | | | **10** | **0-3** | | | | | **10-13** | |

| Наименование раздела | Формы и вид контроля | Рейтинговые показатели | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | I текущий контроль | Дополнительные баллы к ТК1 | II текущий контроль | Дополнительные баллы к ТК2 | III текущий контроль | Дополнительные баллы к ТК3 | IV текущий контроль | Дополнительные баллы к ТК4 | Итого | Промежуточная аттестация |
| **защиты информации (КСЗИ)»** | | | | | | | | | | | |
| Тест или письменный опрос | | | | 2 | | | | | | | |
| Защита лабораторной работы | | | | 8 | | | | | | | |
| **Раздел 4. Идентификация, аутентификация и управление доступом** | **ТК3** | | | | | **13** | **0-2** | | | **13-15** | |
| Тест или письменный опрос | | | | | | 1 | | | | | |
| Защита лабораторной работы | | | | | | 4 | | | | | |
| **Раздел 5. Обеспечение безопасности информации в операционных системах** | | | | | | | | | | | |
| Тест или письменный опрос | | | | | | 1 | | | | | |
| Защита лабораторной работы | | | | | | 4 | | | | | |
| **Раздел 6. Средства антивирусной защиты (САВЗ)** | | | | | | | | | | | |
| Тест или письменный опрос | | | | | | 1 | | | | | |
| Защита лабораторной работы | | | | | | 2 | | | | | |

| Наименование раздела | Формы и вид контроля | Рейтинговые показатели | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | I текущий контроль | Дополнительные баллы к ТК1 | II текущий контроль | Дополнительные баллы к ТК2 | III текущий контроль | Дополнительные баллы к ТК3 | IV текущий контроль | Дополнительные баллы к ТК4 | Итого | Промежуточная аттестация |
| **Раздел 7. Обеспечение безопасности информации в компьютерных сетях** | **ТК4** | | | | | | | **11** | **0-3** | **11-14** | |
| Тест или письменный опрос | | | | | | | | 3 | | | |
| Защита лабораторной работы | | | | | | | | 8 | | | |
| **Промежуточная аттестация (зачет)** | **ОМ** | | | | | | | | | | **зачет** |
| Итоговый тест | | | | | | | | | | | 0-45 |

## 2. Оценочные материалы текущего контроля и промежуточной аттестации

Шкала оценки результатов обучения по дисциплине:

| Код компетенции | Код индикатора компетенции | Запланированные результаты обучения по дисциплине | Уровень сформированности индикатора компетенции | | | |
|---|---|---|---|---|---|---|
| | | | Высокий | Средний | Ниже среднего | Низкий |
| | | | от 85 до 100 | от 70 до 84 | от 55 до 69 | от 0 до 54 |
| | | | Шкала оценивания | | | |
| | | | отлично | хорошо | удовлет-ворительно | неудов-летвори-тельно |
| | | | зачтено | | | не зачтено |
| | ОПК-3.2 | знать: | | | | |
| | | основные виды угроз безопасности информации, уязвимостей информационных систем, а также меры и средства противодейств | Уровень знаний в объеме, соответствующем программе подготовки, без ошибок | Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых | Минимально допустимый уровень знаний, имеет место много негрубых | Уровень знаний ниже минимальных требований, имеют место грубые |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | ия атакам на информационные ресурсы при проектировании, разработке и внедрении программного обеспечения информационных систем | | ошибок | ошибок | ошибки |
| | | уметь: | | | | |
| | | разрабатывать проектно-техническую документацию для информационных систем с учетом требований текущего законодательства, нормативно-правовых актов, стандартов и ведущих практик в области информационной безопасности | Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме | Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами | Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме | При решении стандартных задач не продемонстрированы основные умения, имеют место грубые ошибки |
| | | владеть: | | | | |
| | | навыками применения программно-аппаратных средств для анализа защищенности информационных систем для выработки мер противодействия известным угрозам безопасности информации | Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов | Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами | Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами | При решении стандартных задач не продемонстрированы базовые навыки, имеют место грубые ошибки |

Оценка **«зачтено»** выставляется за набор 55 баллов, выставляемых за выполнение лабораторных работ в семестре; решения тестовых заданий на лекциях, решения итоговых тестов по теоретической и практической части.

Оценка **«не зачтено»** выставляется, если количество набранных баллов не достигает порогового значения 55.

### 3. Перечень оценочных средств

Краткая характеристика оценочных средств, используемых при текущем контроле успеваемости и промежуточной аттестации обучающегося по дисциплине:

| Наименование оценочного средства | Краткая характеристика оценочного средства | Описание оценочного средства |
|---|---|---|
| Тест по разделам (темам) | Знание основных понятий темы/раздела/дисциплины | Перечень определений основных понятий темы/дисциплины |
| Отчет по лабораторной работе (ОЛР) | Выполнение лабораторной работы, обработка результатов испытаний, измерений, эксперимента. Оформление отчета, защита результатов лабораторной работы по отчету | Перечень заданий и вопросов для защиты лабораторной работы, перечень требований к отчету |
| Итоговый тест (Тест) | Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося | Комплект тестовых заданий |

### 4. Перечень контрольных заданий или иные материалы, необходимые для оценки знаний, умений и навыков, характеризующих этапы формирования компетенций в процессе освоения дисциплины

*Пример задания*

**Для текущего контроля ТК1:**

Проверяемая компетенция: ОПК-3.2 Способен применять современные информационные технологии при решении задач профессиональной деятельности

| **Вопрос** | **Варианты ответа** | **Ответ** |
|---|---|---|
| Какие из перечисленных компонентов информационной системы могут выступать в роли субъектов? | **пользователи** | |
| | **активные программы** | |
| | **процессы** | |
| | коммутационное оборудование | |
| | линии передачи информации | |

| Вопрос | Варианты ответа | Ответ |
|---|---|---|
| Способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты | **неотказуемость** | |
| | подлинность | |
| | аутентичность | |
| | адекватность | |
| | целостность | |
| Свойство информационной системы, обусловливающее возможность реализации угрозы безопасности обрабатываемой в ней информации | **уязвимость безопасности информации** | |
| | угроза безопасности информации | |
| | риск информационной безопасности | |
| | атака на компьютерную систему | |
| | инцидент информационной безопасности | |
| Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию – это | **защита информации** | |
| | информационная безопасность | |
| | управление безопасностью информации | |
| | менеджмент информационной безопасности | |
| Электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом | **простая электронная подпись** | |
| | усиленная электронная подпись | |
| | усиленная квалифицированная электронная подпись | |
| | усиленная неквалифицированная электронная подпись | |
| | усиленная простая электронная подпись | |
| | простая неквалифицированная электронная подпись | |
| Какое из перечисленных сетевых устройств может выполнять функции межсетевого экрана? | концентратор | |
| | **маршрутизатор** | |
| | коммутатор 3 уровня | |
| | ретранслятор | |
| | коммутатор | |
| | медиаконвертер | |
| Среди перечисленных пунктов выберите действия, для совершения которых должна быть предназначена программа, чтобы считаться вредоносной (согласно определению вредоносной программы из Уголовного кодекса РФ) | несанкционированное распространение информации | |
| | вывод из строя компонентов ИС | |
| | **несанкционированное уничтожение информации** | |
| | поиск уязвимостей в ИС | |
| | **нейтрализация средств защиты компьютерной информации** | |
| К какой группе угроз информационной безопасности относится | программные | |
| | аппаратные | |

| Вопрос | Варианты ответа | Ответ |
|---|---|---|
| дезинформация, сокрытие или искажение информации | **информационные** | |
| | системные | |
| | внешние | |
| Особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используют-ся методы, средства и технологии силового воздействия на информационную сферу этих государств | **Информационная война** | |
| Технология шифрования всей информации, размещенной на жестком диске для защиты от утечки данных, разработанная компанией Microsoft | **BitLocker** | |

**Для текущего контроля ТК2:**

Проверяемая компетенция: ОПК-3.2 Способен применять современные информационные технологии при решении задач профессиональной деятельности

| Вопрос | Варианты ответа |
|---|---|
| Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения | **целостность** |
| | доступность |
| | конфиденциальность |
| | неотказуемость |
| | адекватность |
| Совокупность условий или действий, создающих потенциальную или реально существующую опасность нарушения безопасности информации | **угроза безопасности информации** |
| | риск безопасности информации |
| | уязвимость безопасности информации |
| | атака на информационные ресурсы |
| Установите соответствие между понятиями и определениями:<br>1) процедура распознавания субъекта по его идентификатору<br>2) проверка подлинности субъекта с данным идентификатором<br>3) процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы | активация |
| | верификация |
| | **Авторизация (3)** |
| | **Идентификация (1)** |
| | **Аутентификация (2)** |
| Вредоносная программа, использующая для создания своих копий на других компьютерах сетевые ресурсы и сервисы, называется | спуфер |
| | троянская программа |
| | **червь** |
| | бэкдор |
| | эксплоит |
| Метод криптозащиты, представляющий собой контрольное преобразование информации: из данных неограниченного размера путем выполнения криптографических преобразований вычисляется дайджест фиксированной длины, однозначно соответствующее исходным данным | **хеширование** |
| | криптоанализ |
| | стеганография |
| | электронная подпись |
| | аутентификация |
| Какой вид МЭ дополняет экранирующий маршрутизатор функциями контроля виртуальных соединений и трансляции | экранирующий шлюз |
| | пакетный фильтр |
| | **шлюз сеансового уровня** |

| Вопрос | Варианты ответа |
|---|---|
| внутренних IP-адресов? | прикладной шлюз |
| | экранирующий маршрутизатор |
| Вредоносная программа, реализующая несанкционированные действия, направленные на нарушение безопасности ИС, без создания собственных копий, называется | вредоносной утилитой |
| | сетевым червем |
| | бэкдором |
| | **троянской программой** |
| | флудером |
| К какой группе угроз информационной безопасности относится незаконное копирование данных в информаци-онных системах | аппаратные |
| | системные |
| | внешние |
| | программные |
| | **информационные** |
| Меры защиты информации, относящиеся к организационным мероприятиям | фильтры, экраны на аппаратуру |
| | установка средств антивирусной защиты |
| | электронные ключи на микросхемах |
| | **ограничение доступа лиц в компьютерные помещения** |
| | **хранение носителей и устройств в сейфе** |
| Пользователь, обладающий правом чтения журнала безопасности операционной системы | **аудитор** |

**Для текущего контроля ТК3:**

Проверяемая компетенция: ОПК-3.2 Учитывает при решении задач профессиональной деятельности основные требования к информационной безопасности

| Вопрос | Варианты ответа |
|---|---|
| Какая функция межсетевого экрана позволяет скрывать топологию внутренней сети от внешних пользователей? | кэширование |
| | **трансляция сетевых адресов** |
| | идентификация |
| | администрирование |
| | аутентификация |
| Выберите верные утверждения, касающиеся требований к аудиту событий в ОС | Добавлять записи в журнал аудита может операционная система и администратор |
| | Редактировать или удалять отдельные записи в журнале аудита не может ни один субъект доступа, кроме самой ОС |
| | **Просматривать журнал аудита могут только пользователи, обладающие соответствующей привилегией** |
| | Операционная система не должна поддерживать возможность сохранения журнала аудита перед очисткой в другом файле |
| | **Очищать журнал аудита могут только пользователи-аудиторы** |
| Процедура проверки подлинности входящего в систему объекта (пользователя, процесса или устройства), предъявившего свой идентификатор называется _____ | **аутентификация** |
| Выберите верные утверждения | Симметричное шифрование имеет высокую скорость шифрования, но сложно в реализации |
| | **Симметричное шифрование применимо для шифрования данных произвольной длины** |
| | При симметричном шифровании передача секретного ключа может быть осуществлена по общедоступным каналам связи |
| | Проблема распределения ключей шифрования между пользователями присутствует только для асимметричного шифрования |
| Разложение матрицы доступа по строкам позволяет получить | **мандаты возможностей** |
| | домены безопасности |
| | мандаты полномочий |
| | домены прав доступа |
| | списки прав доступа |
| Протокол SSL используется для защиты информационного обмена | транспортном уровне |
| | **сеансовом уровне** |

| Вопрос | Варианты ответа |
|---|---|
| на | сетевом уровне |
| | прикладном уровне |
| Укажите все свойства сигнатурного анализа, которые можно отнести к его недостаткам: | при успешном определении, лечение «зараженного» объекта часто невозможно |
| | **не позволяет обнаруживать новые вредоносные программы** |
| | **требует значительных усилий по обновлению баз сигнатур** |
| | склонен к большому количеству пропусков вредоносных программ |
| | склонен к большому количеству ложных срабатываний |
| К какой группе угроз информационной безопасности относится перехват информации в линиях связи | **технические** |
| | аппаратные |
| | программные |
| | физические |
| | информационные |
| Выберите меры по защите информации, относящиеся к техническим | **ключ для блокировки клавиатуры** |
| | **электронные ключи на микросхемах** |
| | парольный доступ – задание полномочий пользователя |
| | **фильтры, экраны на аппаратуру** |
| | **устройства аутентификации** |
| При избирательном разграничении доступа данное понятие определяет набор объектов и типов операций, которые могут производиться над каждым объектом операционной системы | матрица доступа |
| | **домен безопасности** |
| | домен полномочий |
| | матрица мандатов |
| | домен доступа |

**Для текущего контроля ТК4:**

Проверяемая компетенция: ОПК-3.2 Учитывает при решении задач профессиональной деятельности основные требования к информационной безопасности

| Вопрос | Варианты ответа |
|---|---|
| На каких уровнях модели OSI формируются виртуальные защищенные каналы передачи данных? | **сеансовый** |
| | **канальный** |
| | представления |
| | **сетевой** |
| | прикладной |
| Метод обнаружения вредоносных программ, суть которого заключается в поиске участков кода исполняемого объекта, отвечающих за конкретные вредоносные действия, называется | комплексным анализом |
| | методом точного поиска |
| | эвристическим анализом |
| | **сигнатурным анализом** |
| | методом эмуляции кода |
| Название атаки на протоколы аутентификации, в которой пользователь пытается выдать себя за другого с целью получения полномочий и возможности действий от лица другого пользователя | **маскарад** |
| Информация в электронной форме, которая присоединена к другой информации в электронной форме или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию | сертификат ключа проверки электронной подписи |
| | **электронная подпись** |
| | ключ электронной подписи |
| | квалифицированный сертификат |
| | ключ проверки электронной подписи |
| | **Симметричное шифрование применимо для шифрования данных произвольной длины** |
| | При симметричном шифровании передача секретного ключа может быть осуществлена по общедоступным каналам связи |
| | Проблема распределения ключей шифрования между пользователями присутствует только для асимметричного шифрования |
| Вид электронной подписи, позволяющий организовать юридически значимый электронный документооборот с партнерскими компаниями, органами государственной власти и внебюджетными фондами | **квалифицированная электронная подпись** |
| | простая электронная подпись |
| | неквалифицированная электронная подпись |
| | расширенная электронная подпись |
| Взаимная аутентификация обеих сторон в SSL выполняется путем | обмена открытыми ключами симметричного шифрования |
| | **обмена цифровыми сертификатами открытых ключей пользователей (клиента и сервера), заверенными цифровой подписью специальных сертификационных** |

| Вопрос | Варианты ответа |
|---|---|
| | **центров** |
| | обмена открытыми ключами ассимметричного шифрования |
| | обмена случайно сгенерированными паролями |
| К какой группе угроз относится внедрение «вирусов», аппаратных и программных закладок | аппаратные |
| | физические |
| | информационные |
| | технические |
| | **программные** |
| Любой элемент операционной системы, доступ к которому пользователей и других субъектов доступа может быть произвольно ограничен (если ответ состоит из больше чем одного слова, напишите слова через пробел) | **объект доступа** |
| Субъект, которому принадлежит объект операционной системы и который несет ответственность за конфиденциальность содержащейся в объекте информации, а также за целостность и доступность объекта | **владелец** |
| Средство защиты, используемое в ОС Windows для снижения риска установки вредоносным ПО нежелательной программы или внесения опасных изменений в систему. | Windows Filrewall |
| | Action Center |
| | Windows Filtering Platform |
| | PowerShell |
| | **User Account Control** |

**Для промежуточной аттестации:**

Примеры заданий:

1. Дано:

- допустимая вероятность подбора пароля злоумышленником 0,0277972
- скорость подбора пароля злоумышленником 493 паролей(-я) в минуту
- срок действия пароля 17 дней(-я)
- мощность алфавита пароля 49 символов

Найти длину пароля, соответствующую заданным условиям.

2. Дано:

- допустимая вероятность подбора пароля злоумышленником 0,0000148
- скорость подбора пароля злоумышленником 493 паролей(-ля,-ль) в минуту

- срок действия пароля 1 недель(-я, -и)
- мощность алфавита пароля 49 символов

Найти:

- длину пароля, соответствующую заданным условиям.

Ответ должен быть целым числом.

3. Дан зашифрованный текст "бшъуэтъвчьттйд"

Какое ключевое слово было использовано, если исходный текст "аутентификация".

4. Алиса передала Бобу открытый ключ (7,143). Боб ответил Алисе зашифрованным сообщением "135".

Ева перехватила сообщение и произвела на него успешную атаку.

Напишите в качестве ответа исходное сообщение Боба (число без кавычек).

5. Боб получил от Алисы три числа: p = 19, g = 5, A = 6. Боб выбрал свой закрытый ключ b = 7 и отправил Алисе открытый ключ B, а также рассчитал общий секретный ключ K. Рассчитайте B и K.

Ответ запишите без пробелов числами через запятую в формате: B,K

6. Распространение влияния одного знака открытого текста на много знаков шифртекста, что позволяет скрыть статистические свойства открытого текста называется _____

7. _____ - предполагает использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифрованного текстов

8. Проявление зависимости всех выходных битов шифротекста от каждого входного бита открытого текста называется _____ эффектом

9. Установите соответствие между типами криптосистем и видами криптографических преобразований

| | |
|---|---|
| 1) бесключевые | a) хеширование |
| 2) одноключевые | b) симметричное шифрование |
| 3) двухключевые | c) асимметричное шифрование |

10. Установите соответствие стандартов шифрования и количества используемых в них раундов шифрования

| | |
|---|---|
| 1) AES128 | a) 10 раундов |
| 2) AES192 | b) 12 раундов |
| 3) AES256 | c) 14 раундов |
| 4) DES | d) 16 раундов |
| 5) 3DES | e) 24 раунда |
| | f) 48 раундов |