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

**АКТУАЛИЗИРОВАНО**
**решением ученого совета ИАТЭ**
**протокол №9 от 28.04.2026**

УТВЕРЖДАЮ
Директор
Института теплоэнергетики

Подписан: ФГБОУ ВО «КГЭУ», КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСИЙ УНИВЕРСИТЕТ
Владелец: Гапоненко Сергей Олегович, Директор института атомной и тепловой энергетики,
Сертификат: 22106E380CE806A24F5558F0019C947E
Действителен с 25.02.2026 по 27.02.2027

_____ С.О.Гапоненко
«_30__»_____05_____ 2023 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.11.03 Основы информационной безопасности

Направление подготовки — 13.03.03 Энергетическое машиностроение

Квалификация — Бакалавр

г. Казань, 2023

Программу разработал(и):

| Наименование кафедры | Должность, уч. степень, уч. звание | ФИО разработчика |
|---|---|---|
| ЦСМ | доцент, к.т.н., доцент | Косулин В.В. |

| Согласование | Наименование подразделения | Дата | № протокола | Подпись |
|---|---|---|---|---|
| Одобрена | ЦСМ | 19.05.2023 | 5 | _____ Зав.каф., к.ф-м.н., доц. Смирнов Ю.Н. |
| Согласована | ЭМС | 22.05.2023 | 12 | _____ Зав.каф., д.т.н., доц. Мингалеева Г. Р. |
| Согласована | Учебно-методический совет ИТЭ | 30.05.2023 | 9 | _____ Директор, к.т.н., доц. Гапоненко С.О. |
| Одобрена | Ученый совет ИТЭ | 30.05.2023 | 9 | _____ Директор, к.т.н., доц. Гапоненко С.О. |

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

Целью освоения дисциплины Б1.О.11.03. "Основы информационной безопасности" является формирования у студентов знаний и навыков по вопросам информационной безопасности, а также навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах организаций и учреждений.

Задачами дисциплины являются: получение базовых теоретических представлений о современных организационных и технических методах защиты информации, а также технических средствах защиты компьютерной информации информационных систем организаций и учреждений.

Компетенции и индикаторы, формируемые у обучающихся:

| Код и наименование компетенции | Код и наименование индикатора |
|---|---|
| ОПК-1. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности | ОПК-1.2. Владеет навыками применения цифровых технологий для решения задач профессиональной деятельности с учетом основных требований информационной безопасности |

## 2. Место дисциплины в структуре ОП

Предшествующие дисциплины (модули), практики, НИР, др.:

Б1.О.11.01. Информационные технологии

Б1.О.11.02. Алгоритмизация и программирование

Последующие дисциплины (модули), практики, НИР, др.:

Б1.О.11.04. Программное обеспечение и программирование в профессиональной деятельности

## 3. Структура и содержание дисциплины

### 3.1. Структура дисциплины

Для очной формы обучения

| Вид учебной работы | Всего ЗЕ | Всего часов | Семестр(ы) | | |
|---|---|---|---|---|---|
| | | | 4 | 5 | 6 |
| ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ | 2 | 72 | 2 | | |
| КОНТАКТНАЯ РАБОТА* | 1,00 | 36 | 36 | | |
| АУДИТОРНАЯ РАБОТА | 0,88 | 32 | 32 | | |
| Лекции | 0,44 | 16 | 16 | | |
| Практические (семинарские) занятия | 0 | 0 | 0 | | |
| Лабораторные работы | 0,44 | 16 | 16 | | |
| САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ | 1,12 | 40 | 40 | | |
| Проработка учебного материала | 1,12 | 40 | 40 | | |
| Курсовой проект | 0 | 0 | 0 | | |
| Курсовая работа | 0 | 0 | 0 | | |
| Подготовка к промежуточной аттестации | 0 | 0 | 0 | | |
| Промежуточная аттестация: | | | З | | |
| | | | – | | |

### 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. Основные понятия и анализ угроз информационной безопасности | 10 | 6 | 8 | 0 | 12 | ТК1 | ОПК-1.2. ЗУВ |
| Раздел 2. Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ. | 6 | 2 | 0 | 0 | 4 | ТК2 | ОПК-1.2. З |
| Раздел 3. Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности | 6 | 2 | 0 | 0 | 4 | ТК3 | ОПК-1.2. З |
| Раздел 4. Инженерно-техническая защита информации | 24 | 4 | 8 | 0 | 12 | ТК4 | ОПК-1.2. ЗУВ |
| Раздел 5. Организационно-правовое обеспечение защиты информации | 10 | 2 | 0 | 0 | 8 | ТК5 | ОПК-1.2. З |
| Зачет | 0 | 0 | 0 | 0 | 0 | **ОМ 1** | **ОПК-1.2. ЗУВ** |
| **Итого за 4 семестр** | **72** | **16** | **16** | **0** | **40** | | |

### 3.3. Содержание дисциплины

Раздел 1. Основные понятия и анализ угроз информационной безопасности.

Тема 1.1. Основные понятия информационной безопасности и защиты информации.

Основные термины и определения. Обеспечение информационной безопасности компьютерных систем. Виды угроз. Три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной (случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные

Тема 1.2. Политика информационной безопасности

Основные понятия политики безопасности. Структура политики безопасности. Разработка политики организации безопасности организации.

Тема 1.3. Стандарты информационной безопасности

Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем Министерства обороны США – «Оранжевая книга». Европейские критерии безопасности информационных технологий. Федеральные критерии безопасности. Канадские критерии безопасности компьютерных систем. ГОСТ Р ИСО/МЭК 15408-2002, как аутентичный вариант общих критериев безопасности ИТ. Функциональные требования безопасности. Требования доверия к безопасности. Стандарты ISO/IEC 17799: 2002 (BS 7799:2000). Стандарты по менеджменту информационной безопасности ISO/IEC 27001-27040. Немецкие стандарты BSI. Стандарты SysTrust, SCORE, GIAC. Стандарты для беспроводных сетей. Отечественные стандарты информационной безопасности. Стандарты обеспечение информационной безопасности организаций банковской системы. Российской Федерации. ГОСТ Р 57580.1-2017 и ГОСТ Р 57580.2 – 2018. Стандарты информационной безопасности в Интернете (IETF, RFC)

Раздел 2. Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ

Органы, обеспечивающие национальную безопасность РФ, цели, задачи. Национальные интересы РФ в информационной сфере. Приоритетные направления в области защиты информации в РФ. Тенденции развития информационной политики государств и ведомств. Государственная тайна.

Раздел 3. Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности

Общие положения. Концептуальные документы в области информационной безопасности. Важнейшие федеральные нормативные правовые акты. Законы, касающиеся охраны интеллектуальной собственности. Положения Гражданского кодекса РФ по защите информации. Международное сотрудничество. Кодекс об административных правонарушениях. Уголовный кодекс и защита информации. Основные подзаконные акты в области информационной безопасности. Указы Президента РФ, постановления Правительства РФ, ведомственная нормативная база.

Раздел 4. Инженерно-техническая защита информации

Понятие криптографии. Критерий надежности шифрования. Основные криптографические приемы: блочное шифрование, схема поточного шифрования. Симметричные криптосистемы шифрования. Ассиметричные криптосистемы шифрования. Функции хэширования. Основные процедуры цифровой подписи. Управление криптоключами. Идентификация, аутентификация и управление доступом: методы аутентификации, использующие пароли, строгая аутентификация, биометрическая аутентификация. Вредоносные закладки (ВЗ): определение, разновидности. Разрушающие действия закладок Особенности взаимодействия с программно-аппаратными средствами защиты. Методика применения средств борьбы с вредоносными закладками на этапе эксплуатации систем. Системы разграничения доступа и защиты от ВЗ. Предупреждение и минимизация последствий воздействия ВЗ. Краткая характеристика мер защиты: юридические, административные и организационные, аппаратно-программные. Компьютерные вирусы. Классификация. Жизненный цикл. Основные каналы распространения вирусов и других вредоносных программ. Средства борьбы с вирусами: краткая характеристика популярных антивирусных программ. Средства защиты от копирования. Примеры средств и технологий. Вопросы правовой защиты

Раздел 5. Организационно-правовое обеспечение защиты информации

Сущность и роль организационно-правовых аспектов информационной безопасности. Человек как главное звено в системе защиты информации и как злоумышленник. Нормативная правовая база информационной безопасности. Закон РФ “Об информации, информационных технологиях и о защите информации”. Виды и категории информации ограниченного доступа: государственная и другие виды тайн. Закон РФ “О государственной тайне”, “О коммерческой тайне”, “О персональных данных”, “О национальной платежной системе”, “О безопасности критической информационной инфраструктуры Российской Федерации”. Государственная система лицензирования и сертификации деятельности в области защиты информации. Указ Президента РФ “О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации”. Закон РФ “Об электронной цифровой подписи”. Уголовно- правовое регулирование защиты информации.

### 3.4. Тематический план практических занятий

Данный вид работы не предусмотрен учебным планом.

### 3.5. Тематический план лабораторных работ

| № п/п | Наименование лабораторных работ | Номер раздела | Продолжительность, час. |
|---|---|---|---|
| 1 | Настройка политики безопасности операционной системы | 1 | 4 |
| 2 | Организация защиты документов средствами пакета Microsoft Office | 1 | 4 |
| 3 | Настройка параметров безопасности интернет-браузера | 4 | 4 |

| № п/п | Наименование лабораторных работ | Номер раздела | Продолжительность, час. |
|---|---|---|---|
| 4 | Шифрование информации методом полиалфавитной замены. Построение и использование матрицы Вижинера | 4 | 4 |

### 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 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 | удовлетворительно | неудовлетворительно |
| | | | зачтено | | | не зачтено |
| ОПК-1 | ОПК-1.2 | знать: | | | | |
| | | знать правовые акты в области защиты информации, основные понятия и угрозы информационной безопасности, основные мероприятия по обеспечению информационной безопасности в профессиональной деятельности | знает в совершенстве | знает основные принципы | знает отдельные принципы | имеет представление |
| | | информационно-коммуникационные технологии, применяемые для решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности | знает в совершенстве | знает основные принципы | знает отдельные принципы | имеет представление |

| 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 |
| | | уметь: | | | | |
| | | использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной информации или утраты защищаемой информации | умеет в совершенстве | умеет с некритичными ошибками | дпускает отдельные грубые ошибки | не может без посторонней помощи использовать |
| | | оценивать опасность, связанную с угрозами несанкционированного доступа к информации, намеренной модификации данных и утраты служебной информации | умеет в совершенстве | умеет с некритичными ошибками | дпускает отдельные грубые ошибки | не может без посторонней помощи использовать |
| | | владеть: | | | | |
| | | современными общими способами обеспечения информационной безопасности | владеет в совершенстве | владеет отдельными навыками | владеет отдельными навыками с недочетами | не владеет без посторонней помощи |

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

5.1.1. Основная литература

1. Медведев, В. А., Информационная безопасность. Введение в специальность + еПриложение: Тесты : учебник / В. А. Медведев. — Москва : КноРус, 2023. — 143 с. — ISBN 978—5-406—11334—9. — URL: https://book.ru/boolf948870. — Текст : электронный.

2. 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

3. Защита информации : учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — URL: hnp://new.ibool‹s.ru/bookshelf/361250. - Текст : электронный.

### 5.1.2.Дополнительная литература

1. Крылов, Г. О., Базовые понятия информационной безопасности : учебное пособие / Г. О. Крылов, С. Л. Ларионова, В. Л. Никитина. — Москва : Русайнс, 2023. — 257 с. — ISBN 978-5-466-01996-4. — URL: https://boolc.ru/book/946979. — Текст электронный.

2. Бабаш, А. В., Криптографические методы защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2022. — 189 с. — ISBN 978-5-406- 08880-7. — URL: https://book.ru/book/941751. — Текст : электронный.

3. Организационно-правовое обеспечение информационной безопасности учебное пособие для вузов / А. А. Стрельцов, В. С. Горбатов, Т. А. Полякова [и др.]; под ред. А. А. Стрельцова. - М. : Академия, 2008. - 256 с. - ISBN 978-5-7695-4240-4. - Текст : непосредственный.

4. Информационная безопасность: концептуальные и методологические основы защиты информации : учебное пособие / А.А. Малюк. - М. : Горячая линия - Телеком, 2004. - 280 с. - Текст : непосредственный.

### 5.2 Информационное обеспечение

5.2.1. Электронные и интернет-ресурсы

| № п/п | Наименование электронных и интернет-ресурсов | Ссылка |
|---|---|---|
| 1 | Электронно-библиотечная система «Лань» | https://e.lanbook.com |
| 2 | Электронно-библиотечная система «ibooks.ru » | https://books.n |

5.2.2. Профессиональные базы данных / Информационно-справочные системы

| № п/п | Наименование профессиональных баз данных, информационно-справочных систем | Адрес | Режим доступа |
|---|---|---|---|
| 1 | Российская национальная библиотека | http://nlr.ru/ | http://nlr.ru/ |
| 2 | Общероссийский математический портал | http://www.mathnet.ru/ | http://www.mathnet.ru/ |
| 3 | КиберЛенинка | В https://cyberleninka.ru/ | В https://cyberleninka.ru/ |
| 4 | Национальная электронная библоиотека (НЭБ) | https://rusneb.ru/ | https://rusneb.ru/ |
| 5 | Техническая библиотека | http://techlibrary.ru | http://techlibrary.ru |
| 6 | ИСС «Кодекс» / «Техэксперт» | http://app.kgeu.local/Home/Apps | http://app.kgeu.local/Home/Apps |
| 7 | «Консультант плюс» | http://www.consultant.ru/ | http://www.consultant.ru/ |
| 8 | «Гарант» | http://www.garant.ru/ | http://www.garant.ru/ |

5.2.3. Лицензионное и свободно распространяемое программное обеспечение дисциплины

| № п/п | Наименование программного обеспечения | Способ распространения (лицензионное/свободно) | Реквизиты подтверждающих документов |
|---|---|---|---|
| 1 | Windows 7 Профессиональная (Pro) | Пользовательская операционная система | ЗАО "СофтЛайнТрейд" №2011.25486 от 28.11.2011 Неискл. право. Бессрочно |
| 2 | Windows 7 Профессиональная (Starter) | Пользовательская операционная система | ЗАО "СофтЛайнТрейд" №2011.25486 от 28.11.2011 Неискл. право. Бессрочно |

## 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 |

| Наименование вида учебной работы | Наименование учебной аудитории, специализированной лаборатории | Перечень необходимого оборудования и технических средств обучения |
|---|---|---|
| Лабораторные работы | Компьютерный класс с выходом в Интернет Д-418, Д-420, Д-424, Д-427 | Специализированная учебная мебель, технические средства обучения (мультимедийный проектор, моноблоки 25 ше.), лицензионное программное обеспечение |
| | Компьютерный класс с выходом в Интернет В-600а | Специализированная учебная мебель на 30 посадочных мест, 30 компьютеров, технические средства обучения (мультимедийный проектор, компьютер (ноутбук), экран), видеокамеры, программное обеспечение |
| Самостоятельная работа | Компьютерный класс с выходом в Интернет В-600а | Специализированная учебная мебель на 30 посадочных мест, 30 компьютеров, технические средства обучения (мультимедийный 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 выпускающая кафедра) |
|---|---|---|---|---|---|
| 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

Б1.О.11.03. Основы информационной безопасности

*(Наименование дисциплины в соответствии с учебным планом)*

г. Казань, 2023

Оценочные материалы по дисциплине, 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 4

| 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 | Итого | Промежуточная аттестация |
| Раздел 1. Основные понятия и анализ угроз информационной безопасности | **ТК1** | **15** | **15** | | | | | **15-30** | |
| Письменный опрос | | 5 | 5 | | | | | | |
| Защита лабораторной работы | | 5 | 10 | | | | | | |
| Отчет по самостоятельной работе | | 5 | | | | | | | |
| Раздел 2. Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ | **ТК1** | **10** | | | | | | **10-15** | |
| Письменный опрос | | 5 | 5 | | | | | | |
| Отчет по самостоятельной работе | | 5 | | | | | | | |
| Раздел 3. Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности | **ТК1** | **10** | | | | | | **10-15** | |
| Письменный опрос | | 5 | 5 | | | | | | |
| Отчет по самостоятельной работе | | 5 | | | | | | | |
| Раздел 4. Инженерно-техническая защита информации | **ТК2** | | | **15** | **15** | | | **15-30** | |
| Письменный опрос | | | | 5 | 5 | | | | |
| Защита лабораторной работы | | | | 5 | 10 | | | | |
| Отчет по самостоятельной работе | | | | 5 | | | | | |
| Раздел 5. Организационно-правовое обеспечение защиты информации | **ТК3** | | | | | **5** | **5** | **5-10** | |
| Письменный опрос | | | | | | 3 | 5 | | |
| Отчет по самостоятельной работе | | | | | | 2 | | | |
| **Промежуточная аттестация (зачет)** | **ОМ** | | | | | | | | **0-45** |
| Задание промежуточной аттестации | | | | | | | | | 0-15 |
| В письменной форме по билетам | | | | | | | | | 0-30 |

## 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-летворительно |
| | | | зачтено | | | не зачтено |
| ОПК-1 | ОПК-1.2 | знать: | | | | |
| | | знать правовые акты в области защиты информации, основные понятия и угрозы информационной безопасности, основные мероприятия по обеспечению информационной безопасности в профессиональной деятельности | знает в совершенстве | знает основные принципы | знает отдельные принципы | имеет представление |
| | | информационно-коммуникационные технологии, применяемые для решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности | знает в совершенстве | знает основные принципы | знает отдельные принципы | имеет представление |
| | | уметь: | | | | |
| | | использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной информации или утраты защищаемой информации | умеет в совершенстве | умеет с некритичными ошибками | дпускает отдельные грубые ошибки | не может без посторонней помощи использовать |

| 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-летворительно |
| | | | зачтено | | | не зачтено |
| | | оценивать опасность, связанную с угрозами несанкционированного доступа к информации, намеренной модификации данных и утраты служебной информации | умеет в совершенстве | умеет с некритичными ошибками | допускает отдельные грубые ошибки | не может без посторонней помощи использовать |
| | | владеть: | | | | |
| | | современными общими способами обеспечения информационной безопасности | владеет в совершенстве | владеет отдельными навыками | владеет отдельными навыками с недочетами | не владеет без посторонней помощи |

Оценка **«отлично»** выставляется за владение в полной мере понятийным аппаратом дисциплины «Основы информационной безопасности», способность иллюстрировать ответ примерами, фактами, данными научных исследований, применять теоретические знания для решения типовых задач и практических заданий более высокого уровня сложности.

Оценка **«хорошо»** выставляется за владение понятийным аппаратом дисциплины «Основы информационная безопасности», способен иллюстрировать ответ примерами, фактами, применять теоретические знания при решении типовых задач, допускает незначительные ошибки при решении практических заданий более высокого уровня сложности.

Оценка **«удовлетворительно»** выставляется за частичное владение теоретическими основами дисциплины «Основы информационная безопасности», фрагментарную способность иллюстрировать ответ примерами, фактами, в ряде случаев затрудняется применять теоретические знания при решении типовых задач, не всегда способен решить практические задания более высокого уровня сложности.

Оценка **«неудовлетворительно»** выставляется за не соответствие любым трем из перечисленных показателей. Обучающийся демонстрирует отрывоч-

ные, фрагментарные знания, допускает грубые ошибки при решении типовых расчетных задач либо не имеет представления о способе их решения.

**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 |
|---|---|---|
| Конспектирование учебного материала | Краткое текстовое представление переработанной информации | Перечень разделов |
| 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 |
| Собеседование (Сбс) | Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. | Вопросы по разделам дисциплины |
| 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**

*Примерный перечень вопросов для собеседования*

1. Сформулируйте понятие информационной безопасности ИС.
2. Объясните понятия целостности, конфиденциальности и доступности информации.
3. Укажите отличия санкционированного доступа к информации от несанкционированного.
4. Перечислите основные признаки классификации возможных угроз безопасности ИС
5. Дайте краткую характеристику угрозы безопасности, обозначаемой термином «троянский конь».
6. Дайте краткую характеристику угроз безопасности, обозначаемых терминами «вирус» и «червь».
7. Назовите и охарактеризуйте наиболее распространенные виды сетевых.
8. Опишите атаку «человек-в-середине». Какие средства позволяют эффективно бороться с атаками такого типа?

9. Опишите атаку типа «отказ в обслуживании» и распределенную атаку «отказ в обслуживании».

10. Опишите особенности фишинга и фарминга. Укажите меры противодействия этим атакам.

11. Каковы источники нарушений безопасности проводных корпоративных сетей?

12. Назовите основные уязвимости и угрозы беспроводных сетей.

13. Объясните понятие «политика безопасности организации».

14. Какие разделы должна содержать документально оформленная политика безопасности?

15. Какие проблемы решает верхний уровень политики безопасности?

16. Какие задачи решает средний уровень политики безопасности?

17. Каковы особенности нижнего уровня политики безопасности?

18. Сформулируйте обязанности руководителей подразделений, администраторов и пользователей при реализации политики безопасности.

19. Опишите структуру политики безопасности организации.

20. Что представляют собой специализированные политики безопасности?

21. Приведите несколько примеров специализированных политик безопасности с описанием их особенностей.

22. Что представляют собой процедуры безопасности?

23. Приведите несколько примеров процедур безопасности с описанием их особенностей.

24. Перечислите основные этапы разработки политики безопасности организации.

25. Сформулируйте главную задачу стандартов информационной безопасности с позиций производителен и потребителей продуктов информационных технологий, а также специалистов по сертификации этих продуктов.

26. Назовите основные международные стандарты информационной безопасности.

27. Дайте краткую характеристику международного стандарта IS0/IEC 17799:2000 (BS 7799-1:2000).

28. Каковы основные особенности германского стандарта BSI «Руководство но защите информационных технологий для базового уровня защищенности»?

29. Опишите содержание и укажите значение международного стандарта ISO 15408 «Общие критерии безопасности информационных технологий».

30. Перечислите стандарты для беспроводных сетей и дайте их краткую характеристику.

31. Назовите стандарты информационной безопасности для Интернета.

32. Что такое криптография?

33. Дайте определения следующих понятий: криптограмма, криптоалгоритм, криптосистема

34. В чем состоит коренное различие симметричных и асимметричных криптосистем?

35. Опишите две основные процедуры, осуществляемые системой электронной цифровой подписи для подтверждения подлинности цифрового документа.

36. Каким образом комбинированный метод шифрования позволяет сочетать достоинства ассиметричных и симметричных криптосистем? Опишите протокол реализации комбинированного метода шифрования.

37. Что такое вредоносная программа? Охарактеризуйте основные типы вредоносных программ.

38. Укажите существенные отличия компьютерных вирусов от сетевых червей. Опишете основные особенности троянских программ.

39. Опишите два основных подхода к обнаружению вредоносных программ.

40. Как выполняется сигнатурный анализ? Каковы его достоинства и недостатки?

41. Что представляют собой проактивные методы обнаружения? Дайте характеристики двух наиболее популярных подходов.

42. Опишите принцип действия, достоинства и недостатки эвристических анализаторов.

43. Опишите принцип действия, достоинства и недостатки поведенческих блокираторов.

44. Назовите и опишите дополнительные модули антивирусных средств.

45. Каковы дополнительные меры и средства защиты от вредоносных программ, расширяющие возможности антивирусных программ?

46. Опишите меры и средства зашиты от спама.

47. Каковы особенности реализации подсистемы защиты корпоративной информации от вредоносных программ и вирусов?

48. Каковы возможности серии продуктов Kaspersky Open Space Security для зашиты корпоративных сетей от современных интернет-угроз?

**Для текущего контроля ТК1:**

Проверяемая компетенция:

| Код и наименование компетенции | Код и наименование индикатора |
|---|---|
| ОПК-1. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности | ОПК-1.2. Владеет навыками применения цифровых технологий для решения задач профессиональной деятельности с учетом основных требований информационной безопасности |

Тест

| *Вопрос* | *Варианты ответа* |
|---|---|
| Сколько выделено основных составляющих национальных интересов | 3 |
| | 4 |
| | 5 |

| *Вопрос* | *Варианты ответа* |
|---|---|
| Российской Федерации в информационной сфере?. | 6 |
| Активный перехват информации это перехват, который: | заключается в установке подслушивающего устройства в аппаратуру средств обработки информации |
| | основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций |
| | осуществляется путем использования оптической техники |
| | неправомерно использует технологические отходы информационного процесса |
| | осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера |
| Обеспечение национальной безопасности на государственном уровне определяется следующей целью | надежная защита личной и имущественной безопасности |
| | обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий |
| | преодоление конфронтации в обществе, достижение национального согласия |
| | обеспечение признанных международным правом интересов граждан России, проживающих в зарубежных странах |
| | обеспечение суверенитета и территориальной целостности России |
| В стандарте «Оранжевая книга» фундаментальное требование, которое относится к группе Подотчетность | управляющие доступом метки должны быть связаны с объектами |
| | необходимо иметь явную и хорошо определенную систему обеспечения безопасности |
| | индивидуальные субъекты должны идентифицироваться |
| | вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований |
| | гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений |
| Защита информации от несанкционированного воздействия это деятельность по предотвращению | получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации |
| | воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации |
| | воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений |
| | неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа |

| *Вопрос* | *Варианты ответа* |
|---|---|
| | несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации |
| Защита информации это | процесс сбора, накопления, обработки, хранения, распределения и поиска информации |
| | преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа |
| | получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств |
| | совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям |
| | деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё |
| Пассивный перехват информации это перехват, который | заключается в установке подслушивающего устройства в аппаратуру средств обработки информации |
| | основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций |
| | неправомерно использует технологические отходы информационного процесса |
| | осуществляется путем использования оптической техники |
| | осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера |
| Обеспечение национальной безопасности на государственном уровне определяется следующей целью | надежная защита личной и имущественной безопасности |
| | обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий |
| | преодоление конфронтации в обществе, достижение национального согласия |
| | обеспечение социально-политической и экономической стабильности страны |
| | обеспечение признанных международным правом интересов граждан России, проживающих в зарубежных странах |
| К источникам защищаемой информации относится | электрические поля |
| | сырье |
| | магнитные поля |
| | электромагнитные поля |
| | элементарные частицы |
| | акустические колебания |
| Естественные угрозы безопасности информации вызваны | деятельностью человека |
| | ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения |
| | воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека |
| | корыстными устремлениями злоумышленников |
| | ошибками при действиях персонала |

| *Вопрос* | *Варианты ответа* |
|---|---|
| Защита информации от непреднамеренного воздействия это деятельность по предотвращению | получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации |
| | воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации |
| | воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений |
| | неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа |
| | несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации |
| Информационные процессы это | процесс сбора, накопления, обработки, хранения, распределения и поиска информации |
| | преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа |
| | получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств |
| | совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям |
| | деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё |
| Аудиоперехват перехват информации это перехват, который | заключается в установке подслушивающего устройства в аппаратуру средств обработки информации |
| | основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций |
| | неправомерно использует технологические отходы информационного процесса |
| | осуществляется путем использования оптической техники |
| | осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера |
| В стандарте «Оранжевая книга» фундаментальное требование, которое относится к группе Гарантии | управляющие доступом метки должны быть связаны с объектами |
| | необходимо иметь явную и хорошо определенную систему обеспечения безопасности |
| | индивидуальные субъекты должны идентифицироваться |
| | вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований |

| *Вопрос* | *Варианты ответа* |
|---|---|
| | контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность |
| К носителям защищаемой информации относится | люди |
| | сырье |
| | черновики и отходы производства |
| | документы |
| | акустические колебания |
| Искусственные угрозы безопасности информации вызваны | деятельностью человека |
| | ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения |
| | воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека |
| | корыстными устремлениями злоумышленников |
| | ошибками при действиях персонала |
| Защита информации от разглашения это деятельность по предотвращению | получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации |
| | воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации |
| | воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений |
| | неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; |
| | несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации |
| Просмотр мусора это перехват информации, который | заключается в установке подслушивающего устройства в аппаратуру средств обработки информации |
| | основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций |
| | неправомерно использует технологические отходы информационного процесса |
| | осуществляется путем использования оптической техники |
| | осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера |
| К основным непреднамеренным искусственным угрозам АСОИ относится | физическое разрушение системы путем взрыва, поджога и т.п. |
| | перехват побочных электромагнитных, акустических и других излучений устройств и линий связи |
| | изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п. |

| *Вопрос* | *Варианты ответа* |
|---|---|
| | чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств |
| | неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы |
| Защита информации от несанкционированного доступа это деятельность по предотвращению | получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации |
| | воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации |
| | воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений |
| | неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа |
| | несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации |
| Доступ к информации это | процесс сбора, накопления, обработки, хранения, распределения и поиска информации |
| | преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа |
| | получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств |
| | совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям |
| | деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё |
| Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется | активный перехват |
| | пассивный перехват |
| | аудиоперехват |
| | видеоперехват |
| | просмотр мусора |
| В международном стандарте «Оранжевая книга» минимальная защита это группа | A |
| | B |
| | C |
| | D |
| | E |
| По характеру воздействия удаленные атаки делятся на | условные и безусловные |
| | атаки с обратной связью и без обратной связи |
| | внутрисегментные и межсегментные |
| | пассивные и активные |

| *Вопрос* | *Варианты ответа* |
|---|---|
| | атаки, которые могут реализовываться на всех семи уровнях – физическом, канальном, сетевом, транспортном, сеансовом, представительном и прикладном |
| Субъект доступа к информации это | физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов |
| | субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации |
| | субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением |
| | субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами |
| | участник правоотношений в информационных процессах |
| Перехват, который осуществляется путем использования оптической техники, называется | активный перехват |
| | пассивный перехват |
| | аудиоперехват |
| | видеоперехват; |
| | просмотр мусора |
| Обеспечение национальной безопасности на уровне гражданского общества определяется следующей целью | надежная защита личной и имущественной безопасности |
| | обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий |
| | повышение эффективности защиты конституционного строя, правопорядка, борьбы с орг. преступностью и коррупцией |
| | преодоление конфронтации в обществе, достижение национального согласия |
| В международном стандарте «Оранжевая книга» индивидуальная защита это группа | A |
| | B |
| | C |
| | D |
| | E |
| По цели воздействия удаленные атаки делятся на | условные и безусловные |
| | атаки с обратной связью и без обратной связи |
| | внутрисегментные и межсегментные |
| | пассивные и активные |
| | атаки в зависимости от нарушения конфиденциальности, целостности и доступности |
| Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется | активный перехват |
| | пассивный перехват |
| | аудиоперехват |
| | видеоперехват |
| | просмотр мусора |
| В международном | A |

| *Вопрос* | *Варианты ответа* |
|---|---|
| стандарте «Оранжевая книга» мандатная защита это группа | B |
| | C |
| | D |
| | E |
| По условию начала осуществления воздействия удаленные атаки делятся на | условные и безусловные |
| | атаки с обратной связью и без обратной связи |
| | внутрисегментные и межсегментные |
| | пассивные и активные |
| | атаки в зависимости от нарушения конфиденциальности, целостности и доступности |
| Собственник информации это | физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов |
| | субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации |
| | субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением |
| | субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами |
| | участник правоотношений в информационных процессах |
| Перехват, который осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера называется | активный перехват |
| | пассивный перехват |
| | аудиоперехват |
| | просмотр мусора |
| | видеоперехват |
| В международном стандарте «Оранжевая книга» верифицированная защита это группа | A |
| | B |
| | C |
| | D |
| | E |
| По наличию обратной связи с атакуемым объектом удаленные атаки делятся на | условные и безусловные |
| | атаки с обратной связью и без обратной связи |
| | внутрисегментные и межсегментные |
| | пассивные и активные |
| | атаки в зависимости от нарушения конфиденциальности, целостности и доступности |
| Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации | источник информации |
| | потребитель информации |
| | уничтожитель информации |
| | носитель информации |
| | обладатель информации |
| Обязательное для | электронное сообщение |

| *Вопрос* | *Варианты ответа* |
|---|---|
| выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя это | распространение информации |
| | предоставление информации |
| | конфиденциальность информации |
| | доступ к информации |
| Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц это | уничтожение информации |
| | распространение информации |
| | предоставление информации |
| | конфиденциальность информации |
| | доступ к информации |
| Возможность получения информации и ее использования это | сохранение информации |
| | распространение информации |
| | предоставление информации |
| | конфиденциальность информации |
| | доступ к информации |
| Процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом | авторизация |
| | аутентификация |
| | обезличивание |
| | деперсонализация |
| | идентификация |
| Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации | авторизация |
| | обезличивание |
| | деперсонализация |
| | аутентификация |
| | идентификация |
| Процесс, а также результат процесса проверки некоторых обязательных параметров пользователя и, при успешности, предоставление ему определённых полномочий на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом | авторизация |
| | идентификация |
| | аутентификация |
| | обезличивание |
| | деперсонализация |
| Несанкционированный доступ к информации это | доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально |
| | работа на чужом компьютере без разрешения его владельца |
| | вход на компьютер с использованием данных другого пользователя |
| | доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей |
| | доступ к СУБД под запрещенным именем пользователя |

| *Вопрос* | *Варианты ответа* |
|---|---|
| Документированная информация, доступ к которой ограничивает в соответствии с законадельством РФ | информация составляющая государственную тайну |
| | информация составляющая коммерческую тайну |
| | персональная |
| | конфиденциальная информация |
| | документированная информация |
| Информационная безопасность обеспечивает… | блокирование информации |
| | искажение информации |
| | сохранность информации |
| | утрату информации |
| | подделку информации |
| Хищение информации – это… | несанкционированное копирование информации |
| | утрата информации |
| | блокирование информации |
| | искажение информации |
| | продажа информации |
| Доступ к информации – это: | обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя |
| | действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц |
| | действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц |
| | информация, переданная или полученная пользователем информационно-телекоммуникационной сети |
| | возможность получения информации и ее использования |
| Обеспечение информационной безопасности есть обеспечение… | независимости информации |
| | изменения информации |
| | копирования информации |
| | сохранности информации |
| | преобразования информации |
| К какому виду мер защиты информации относится утвержденная программа работ в области безопасности | политика безопасности верхнего уровня |
| | политика безопасности среднего уровня |
| | политика безопасности нижнего уровня |
| | принцип минимизации привилегий |
| | защита поддерживающей инфраструктуры |
| Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений | конфиденциальность |
| | целостность |
| | доступность |
| | аутентичность |
| | апеллируемость |
| К функциям информационной безопасности относятся | выявление источников внутренних и внешних угроз |
| | страхование информационных ресурсов |
| | защита государственных информационных ресурсов |
| | подготовка специалистов по обеспечению информационной безопасности |
| | все ответы верны |
| К национальным интересам РФ в информационной сфере относятся | реализация конституционных прав на доступ к информации |
| | защита информации, обеспечивающей личную безопасность |
| | защита независимости, суверенитета, государственной и территориальной целостности |
| | политическая экономическая и социальная стабильность |
| | сохранение и оздоровлении окружающей среды |

| *Вопрос* | *Варианты ответа* |
|---|---|
| Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена | конфиденциальность |
| | целостность |
| | доступность |
| | аутентичность |
| | апеллируемость |
| Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности | комплексное обеспечение информационной безопасности |
| | безопасность АС |
| | угроза информационной безопасности |
| | атака на автоматизированную систему |
| | политика безопасности |
| Наиболее распространенные угрозы информационной безопасности | угрозы целостности |
| | угрозы защищенности |
| | угрозы безопасности |
| | угрозы доступности |
| | угрозы конфиденциальности |
| Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы | комплексное обеспечение информационной безопасности |
| | безопасность АС |
| | угроза информационной безопасности |
| | атака на автоматизированную систему |
| | политика безопасности |
| Состояние защищенности многонационального народа как носителя суверенитета и единственного источника власти | информационная безопасность |
| | безопасность |
| | защита информации |
| | национальная безопасность |
| Свойство данных быть доступными для санкционированного пользования в произвольный момент времени, когда в обращении к ним возникает необходимость | конфиденциальность |
| | целостность |
| | доступность |
| | аутентичность |
| | аппелируемость |
| Гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор | конфиденциальность |
| | целостность |
| | доступность |
| | аутентичность |
| | аппелируемость |
| Гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно тот человек, который заявлен как ее автор и ни кто другой | конфиденциальность |
| | целостность |
| | доступность |
| | аутентичность |
| | аппелируемость |
| Соотнесите интересы в области информационной безопасности: | 1. Национальные интересы |
| | 2. Интересы личности |
| | 3. Интересы государства |
| | 4. Интересы общества |
| | 1. состоят в реализации конституционных прав и свобод, в обеспечении личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии человека и гражданина |

| *Вопрос* | *Варианты ответа* |
|---|---|
| | 2. обеспечиваются институтами государственной власти, осуществляющими свои функции, в том числе во взаимодействии с действующими на основе Конституции РФ и законодательства РФ общественными организациями |
| | 3. состоят в незыблемости конституционного строя, суверенитета и территориальной целостности России, в политической, экономической и социальной стабильности, в безусловном обеспечении законности и поддержании правопорядка, в развитии равноправно го и взаимовыгодного международного сотрудничества |
| | 4. состоят в упрочении демократии, в создании правового, социального государства, в достижении и поддержании общественного согласия, в духовном обновлении России |
| Соотнесите основные понятия в области информационной безопасности | 1. атака |
| | 2. уязвимость АС |
| | 3. угроза безопасности АС |
| | 4. защищенная система |
| | 1. некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы |
| | 2. система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности |
| | 3. возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности |
| | 4. действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы |
| Соотнесите основные виды угроз для АС | 1. угроза нарушения конфиденциальности |
| | 2. угроза отказа служб |
| | 3. угроза нарушения целостности |
| | 1. любое умышленное изменение информации, хранящейся в ВС или передаваемой от одной системы в другую |
| | 2. возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу АС |
| | 3. заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней |
| Соотнесите классификацию угроз по ряду признаков | 1. по природе возникновения |
| | 2. по непосредственному источнику |
| | 3. по степени воздействия на АС |
| | 4. по способу доступа к ресурсам АС |
| | 1. пассивные и активные |
| | 2. направленные на использование прямого стандартного пути доступа к ресурсам и направленные на использование скрытого нестандартного доступа к ресурсам АС |
| | 3. естественные или искусственные |
| | 4. природная среда, человек, санкционированные программные средства и несанкционированные программные средства |
| Что такое сертификация | подтверждение соответствия продукции или услуг установленным требованиям или стандартам |

| *Вопрос* | *Варианты ответа* |
|---|---|
| | подтверждение соответствия продукции, но не услуг установленным требованиям или стандартам |
| | подтверждение соответствия услуг, но не продукции установленным требованиям или стандартам |
| Что такое сертификат? | документ, подтверждающий соответствие средства зашиты информации требованиям по безопасности информации |
| | документ, подтверждающий соответствие средства зашиты информации требованиям по хранению информации |
| | документ, подтверждающий соответствие средства зашиты информации требованиям по обработке информации |
| Как называется лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам? | субъект персональных данных |
| | оператор информационной системы |
| | обладатель информации |
| | субъект информации |

**Вопросы к комплексному заданию ТК1**

1. Что такое информационная безопасность?
2. Перечислите важнейшие аспекты информационной безопасности.
3. Перечислите уровни защиты информации.
4. Охарактеризуйте угрозы информационной безопасности: раскрытия целостности, отказ в обслуживании.
5. Объясните причины компьютерных преступлений.
6. Опишите основные технологии компьютерных преступлений.
7. Перечислите меры защиты информационной безопасности.
8. Перечислите меры предосторожности при работе с целью защиты информации.
9. Опишите основные меры защиты носителей информации.
10. Почему подключение к глобальной компьютерной сети Интернет представляет собой угрозу для информационной безопасности?
11. Опишите, как использование электронной почты создает угрозу информационной безопасности. Какие меры обеспечивают безопасное использование e-mail?
12. Какие существуют международные и российские стандарты в области безопасности компьютерных систем и информационных технологий?
13. Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”).
14. Руководящие документы Гостехкомиссии России.
15. Международные стандарты информационной безопасности. Стандарт ISO/IEC 15408 "Общие критерии". Описание требований безопасности и характеристик угроз.

**Для текущего контроля ТК2:**

Проверяемая компетенция:

| Код и наименование компетенции | Код и наименование индикатора |
|---|---|
| ОПК-1. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности | ОПК-1.2. Владеет навыками применения цифровых технологий для решения задач профессиональной деятельности с учетом основных требований информационной безопасности |

Тест

| *Вопрос* | *Варианты ответа* |
|---|---|
| Какой общий ущерб по данным Института Компьютерной Безопасности нанесли компьютерные вирусы за последние 5 лет, (млрд. долл. США)? | 4 |
| | 34 |
| | 54 |
| | 74 |
| | 94 |
| По данным журнала «Security Magazine», средний размер ущерба от компьютерного мошенничества составляет (долл. США) | 500000 |
| | 1000000 |
| | 1500000 |
| | 2000000 |
| | 2500000 |
| Шифрование информации это | процесс сбора, накопления, обработки, хранения, распределения и поиска информации |
| | преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа |
| | получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств |
| | совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям |
| | деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё |
| По данным Главного информационного центра МВД России количество компьютерных преступлений ежегодно увеличивается в (раза) | 2 |
| | 2,5 |
| | 3 |
| | 3,5 |
| | 4 |
| По данным Главного информационного центра МВД России ежегодный размер материального ущерба от компьютерных преступлений составляет около (млн. рублей) | 6 |
| | 60 |
| | 160 |
| | 600 |
| | 1600 |
| По данным Главного информационного центра МВД России средний ущерб, причиняемый | 7 |
| | 1,7 |
| | 2,7 |

| *Вопрос* | *Варианты ответа* |
|---|---|
| потерпевшему от 1 компьютерного преступления, равен (млн. рублей) | 3,7 |
| | 4,7 |
| Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе, по сети интернет | идентификация |
| | аутентификация |
| | авторизация |
| | экспертиза |
| | шифрование |
| Для безопасной передачи данных по каналам интернет используется технология | www |
| | dicom |
| | vpn |
| | ftp |
| | xml |
| Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа | антивирус |
| | замок |
| | брандмауэр |
| | криптография |
| | экспертная система |
| Процедура, проверяющая, имеет ли пользователь с предъявленным идентификатором право на доступ к ресурсу это | идентификация |
| | аутентификация |
| | стратификация |
| | регистрация |
| | авторизация |
| Пароль пользователя должен | содержать цифры и буквы, знаки препинания и быть сложным для угадывания |
| | содержать только цифры |
| | содержать только буквы |
| | иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.) |
| | быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д. |
| Пластиковая карточка, содержащая чип для криптографических вычислений и встроенную защищенную память для хранения информации | токен |
| | password |
| | пароль |
| | login |
| | смарт-карта |
| Устройство для идентификации пользователей, представляющее собой | токен |
| | автономный токен |

| *Вопрос* | *Варианты ответа* |
|---|---|
| мобильное персональное устройство, напоминающие маленький пейджер, не подсоединяемые к компьютеру и имеющие собственный источник питания | USB-токен |
| | устройство iButton |
| | смарт-карта |
| Доступ пользователя к информационным ресурсам компьютера и / или локальной вычислительной сети предприятия должен разрешаться только после: | включения компьютера |
| | идентификации по логину и паролю |
| | запроса паспортных данных |
| | запроса доменного имени |
| | запроса ФИО |
| Электронные замки предназначены для … | обеспечения доверенной загрузки компьютера и контроля целостности файлов в системах |
| | сканирования отпечатков пальцев |
| | проверки скорости и загрузки файлов |
| | общего контроля |
| | идентификации пользователя |
| Электронные замки предназначены для: | хранения большого объема конфиденциальной информации |
| | защиты периметра корпоративной сети |
| | надежной аутентификации и идентификации пользователей |
| | блокирования компьютера во время отсутствия пользователя на рабочем месте |
| Для защиты от злоумышленников необходимо использовать | системное программное обеспечение |
| | прикладное программное обеспечение |
| | антивирусные программы |
| | компьютерные игры |
| | музыку, видеофильмы |
| Аппаратные модули доверенной загрузки «АККОРД-АМДЗ» представляют собой… | аппаратный контролер |
| | электронный замок |
| | система контроля |
| | сетевой адаптер |
| | копировальный аппарат |
| Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя, который имеет следующее название | токен |
| | password |
| | пароль |
| | login |
| | смарт-карта |
| Чтобы подписать сообщение электронной цифровой подписью, используются | открытый ключ отправителя |
| | открытый ключ получателя |
| | закрытый ключ отправителя |
| | закрытый ключ получателя |
| Какова последовательность подписания сообщений с помощью ЭЦП? | вычисляется хэш, затем хэш зашифровывается |
| | сообщение зашифровывается, после чего результат хэшируется |
| | при подписании сообщение зашифровывается, при проверке вычисляется хэш |

| *Вопрос* | *Варианты ответа* |
|---|---|
| | вычисляется хэш исходного сообщения, после чего оно зашифровывается |
| В чем заключается такое свойство функции хэширования *H* как стойкость к коллизиям первого рода? | для любого хэша h должно быть практически невозможно вычислить или подобрать такое x, что H(x) = h |
| | должно быть практически невозможно вычислить или подобрать любую пару различных сообщений x и y для которых H(x) = H(y) |
| | длина хэша должна быть фиксированной независимо от длины входного сообщения |
| Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются | компаньон - вирусами |
| | черви |
| | паразитические |
| | призраки |
| | стелс-вирусы |
| Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется | ревизором |
| | иммунизатором |
| | сканером |
| | доктора и фаги |
| Указать недостатки, имеющиеся у антивирусной программы ревизор | неспособность поймать вирус в момент его появления в системе |
| | небольшая скорость поиска вирусов |
| | невозможность определить вирус в новых файлах |
| | все варианты верны |
| К достоинствам технических средств защиты относятся | регулярный контроль |
| | создание комплексных систем защиты |
| | степень сложности устройства |
| | все варианты верны |
| В классификацию вирусов по способу заражения входят | опасные |
| | файловые |
| | резидентные |
| | загрузочные |
| | файлово-загрузочные |
| | нерезидентные |
| К вирусам изменяющим среду обитания относятся: | черви |
| | студенческие |
| | полиморфные |
| | спутники |
| Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются | компаньон - вирусами |
| | черви |
| | стелс - вирусы |
| | макровирусы |
| | призраки |
| К вирусам не изменяющим среду обитания относятся | черви |
| | стелс-вирусы |
| | полиморфные |
| | спутники |
| Некоторое секретное количество информации, известное | идентификатор пользователя |

| *Вопрос* | *Варианты ответа* |
|---|---|
| только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации – это …. | пароль пользователя |
| | учетная запись пользователя |
| | парольная система |
| Исследование возможности расшифрования информации без знания ключей | криптология |
| | криптография |
| | криптоанализ |
| | взлом |
| | несанкционированный доступ |
| Хранение паролей может осуществляться | в виде сверток |
| | в открытом виде |
| | в закрытом виде |
| | в зашифрованном виде |
| | все варианты ответа верны |
| Соотнесите основные методы получения паролей | 1. метод тотального перебора |
| | 2. словарная атака |
| | 3. получение паролей из самой системы на основе программной и аппаратной реализации конкретной системы |
| | 4. проверка паролей, устанавливаемых в системах по умолчанию |
| | 1. для перебора используется словарь наиболее вероятных ключей |
| | 2. двумя возможностями выяснения пароля являются: несанкционированный доступ к носителю, содержащему пароли, либо использование уязвимостей |
| | 3. опробываются все ключи последовательно, один за другим |
| | 4. пароль, установленный фирмой-разработчиком по умолчанию, остается основным паролем в системе |
| Соотнесите функции, выполняемые техническими средствами защиты | 1. внешняя защита |
| | 2. опознавание |
| | 3. внутренняя защита |
| | 1. защита от воздействия дестабилизирующих факторов, проявляющихся непосредственно в средствах обработки информации |
| | 2. защита от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств АСОД |
| | 3. специфическая группа средств, предназначенных для опознавания людей по различным индивидуальным характеристикам |
| Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий: | сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания |
| | подтверждена подлинность электронной цифровой подписи в электронном документе |
| | электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи |

| *Вопрос* | *Варианты ответа* |
|---|---|
| | верны все варианты |
| Создание ключей электронных цифровых подписей осуществляется для использования в | информационной системе общего пользования ее участником или по его обращению удостоверяющим центром |
| | корпоративной информационной системе в порядке, установленном в этой системе |
| | верны оба варианты |
| Чем определяется уровень надежности применяемых криптографических преобразований | значением допустимой вероятности неисправностей или сбоев, приводящих к получению злоумышленником дополнительной информации о криптографических преобразованиях |
| | сложностью комбинации символов, выбранных случайным образом |
| | использованием большого числа ключей для шифрования |
| | отношением количества дешифрованной информации к общему количеству шифрованной информации, подлежащей дешифрованию |
| Как иначе называется симметричное шифрование | шифрование с закрытым ключом |
| | шифрование методом Бейтса |
| | шифрование с открытым ключом |
| | шифрование с переменным ключом |
| Какой алгоритм не используется при симметричном шифровании | поточное шифрование |
| | побитовое шифрование |
| | блочное шифрование |
| | алгоритм Эль-Гамаля |
| Что является преимуществом симметричного шифрования | скорость выполнения криптографических преобразований |
| | легкость внесения изменений в алгоритм шифрования |
| | секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа |
| | применение в системах аутентификации (электронная подпись) |
| Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства? | шифр Маркова |
| | шифр Цезаря |
| | шифр Энигма |
| | шифр Бэбиджа |
| Разделы современной криптографии: | симметричные криптосистемы |
| | криптосистемы с открытым ключом |
| | криптосистемы с дублированием защиты |
| | системы электронной цифровой подписи |
| | управление паролями |
| | управление передачей данных |
| | управление ключами |
| Авторизацией называется | процесс, посредством которого идентификация предполагаемой личности проверяется на основе документа, удостоверяющего личность |

| *Вопрос* | *Варианты ответа* |
|---|---|
| | аутентификация основанная на двух разных типах идентификации. |
| | часть идентичности, которая отражает определенную врожденную особенность личности, то есть то что связано с конкретной личностью |
| | Процесс, который дает (или отключает) право доступа к (сетевым) ресурсам |
| Аутентификация - это процесс проверки предполагаемой подлинности личности на основании какого-либо удостоверения личности, которое может быть | что-то, что вы знаете |
| | что-то, что у вас есть |
| | то, чем вы являетесь |
| Двойной защитой называется | аутентификация на основе двух идентификаторов. |
| | аутентификация основана на двух разных типах идентификации |
| | аутентификация, основанная на двух или более различных типах идентификации |
| Перечислите важные учетные записи для пользователя Интернета, где нужно использовать двухэтапную аутентификацию? | учетные записи для входа в банк |
| | учетные записи, содержащие конфиденциальную личную информацию |
| | адреса электронной почты, на которые вы можете заказать напоминания пароля для других веб-сред |
| | учетные записи социальных сетей |
| | учетные записи служб с помощью которых входят в другие веб-службы |
| Алгоритмы шифрования с открытым ключом по-другому называются | асимметричными алгоритмами шифрования |
| | симметричными алгоритмами шифрования |
| | односторонними алгоритмами шифрования |
| | помехоустойчивыми алгоритмами шифрования |
| Асимметричные алгоритмы шифрования по-другому называются | алгоритмами шифрования с открытым ключом |
| | симметричными алгоритмами шифрования |
| | односторонними алгоритмами шифрования |
| | помехоустойчивыми алгоритмами шифрования |
| Математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, называется в криптографии | криптографической функцией |
| | односторонней функцией |
| | функцией Диффи-Хеллмана |
| | функцией Эйлера |
| Односторонние функции, то есть функции, которые относительно легко вычислить, но практически невозможно найти по значению функции соответствующее значение аргумента, можно использовать для | формирования хеш-кодов |
| | шифрования сообщений |
| | формирования цифровой подписи |
| | контроля и исправления ошибок при передаче информации |

| *Вопрос* | *Варианты ответа* |
|---|---|
| Что является особенностью систем шифрования с открытым ключом по сравнению с симметричными системами шифрования? | возможность шифрования как текстовой, так и графической информации |
| | высокая скорость процессов шифрования/расшифрования |
| | использование малого количества вычислительных ресурсов |
| | отсутствие необходимости предварительной передачи секретного ключа по надёжному каналу связи |
| Для решения каких задач можно использовать алгоритмы шифрования с открытым ключом? | для шифрования передаваемых и хранимых данных в целях их защиты от несанкционированного доступа |
| | для формирования цифровой подписи под электронными документами |
| | для распределения секретных ключей, используемых потом при шифровании документов симметричными методами |
| | для помехоустойчивого кодирования передаваемых сообщений |
| Что является недостатком системы шифрования с открытым ключом? | низкая скорость процессов шифрования-расшифрования |
| | необходимость обновления ключа после каждого факта передачи |
| | отсутствие необходимости предварительной передачи секретного ключа по надёжному каналу |
| | необходимость предварительной передачи секретного ключа по надёжному каналу |
| Что называют закрытым ключом в асимметричных методах шифрования? | ключ, который должен храниться в секрете |
| | ключ, который необязательно хранить в секрете |
| | любой ключ, используемый для шифрования или расшифрования |
| | ключ, который используется для выработки имитовставки |
| Что называют открытым ключом в асимметричных методах шифрования? | ключ, который должен храниться в секрете |
| | ключ, который не обязательно хранить в секрете |
| | любой ключ, используемый для шифрования или расшифрования |
| | ключ, который используется для выработки имитовставки |
| Как называется ключ, используемый в асимметричных криптографических алгоритмах, который можно не хранить в секрете? | закрытый ключ |
| | открытый ключ |
| | тайный ключ |
| | явный ключ |
| | ключ шифрования |
| Сколько ключей используется в криптографических алгоритмах с открытым ключом? | 0 |
| | 1 |
| | 2 |
| | 3 |
| | 4 |
| Что общего имеют все методы шифрования с закрытым ключом? | в них для шифрования информации используется один ключ, а для расшифрования – другой ключ |
| | в них для шифрования и расшифрования информации используется один и тот же ключ |
| | в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов |
| | в них для операций шифрования и расшифрования используется два разных ключа – открытый и закрытый |

| *Вопрос* | *Варианты ответа* |
|---|---|
| Укажите требования к алгоритмам шифрования с открытым ключом | вычислительно невозможно создавать пару (открытый ключ, закрытый ключ) |
| | вычислительно невозможно зашифровать сообщение открытым ключом |
| | вычислительно невозможно, зная открытый ключ, определить соответствующий закрытый ключ |
| | вычислительно невозможно, зная только открытый ключ и зашифрованное сообщение, восстановить исходное сообщение |
| Укажите требования к алгоритмам шифрования с открытым ключом | вычислительно легко зашифровать сообщение открытым ключом |
| | вычислительно легко расшифровать сообщение, используя закрытый ключ |
| | вычислительно невозможно, зная открытый ключ, определить соответствующий закрытый ключ |
| | вычислительно невозможно, зная только открытый ключ и зашифрованное сообщение, восстановить исходное сообщение |
| Какие ключи и как должны применяться при использовании асимметричных криптографических алгоритмов для шифрования передаваемых данных? | отправитель шифрует сообщение открытым ключом получателя, а получатель расшифровывает сообщение своим закрытым ключом |
| | отправитель шифрует сообщение закрытым ключом получателя, а получатель расшифровывает сообщение своим открытым ключом |
| | отправитель шифрует сообщение своим открытым ключом, а получатель расшифровывает сообщение закрытым ключом отправителя |
| | отправитель шифрует сообщение своим закрытым ключом, а получатель расшифровывает сообщение открытым ключом отправителя |
| Каким требованиям должна удовлетворять электронная цифровая подпись? | подпись воспроизводится только одним лицом, а подлинность ее может быть удостоверена многими |
| | подпись воспроизводится многими лицами, а ее подлинность может быть удостоверена только одним лицом |
| | подпись неразрывно связывается с данным сообщением и не может быть перенесена на другой документ |
| | подпись не связывается с конкретным сообщением и может быть перенесена на другой документ |
| Каким требованиям должна удовлетворять электронная цифровая подпись? | после того, как документ подписан, его невозможно изменить |
| | после того, как документ подписан, его можно изменять |
| | подпись неразрывно связывается с данным сообщением и не может быть перенесена на другой документ |
| | подпись не связывается с конкретным сообщением и может быть перенесена на другой документ |
| Каким требованиям должна удовлетворять электронная цифровая подпись? | от поставленной подписи невозможно отказаться, то есть лицо, подписавшее документ, не сможет потом утверждать, что не ставило подпись |
| | подпись воспроизводится многими лицами, а ее подлинность может быть удостоверена только одним лицом |

| *Вопрос* | *Варианты ответа* |
|---|---|
| | подпись неразрывно связывается с данным сообщением и не может быть перенесена на другой документ |
| | подпись не связывается с конкретным сообщением и может быть перенесена на другой документ |
| Для чего предназначен центр сертификации ключей? | для регистрации абонентов |
| | для изготовления сертификатов открытых ключей |
| | для выделения специальных каналов связи абонентам |
| | для хранения изготовленных сертификатов |
| | для поддержания в актуальном состоянии справочника действующих сертификатов |
| | для выпуска списка досрочно отозванных сертификатов |
| Как называется структура в составе большой сети связи, занимающаяся генерированием ключей, их хранением и архивированием, заменой или изъятием из обращения старых и ненужных ключей? | устройство распределения ключей |
| | центр закрытого шифрования |
| | центр распределения ключей |
| | центр открытого шифрования |
| Каким свойствами должен обладать сертификат открытого ключа? | каждый пользователь центра сертификации, имеющий доступ к открытому ключу центра, может извлечь открытый ключ, включенный в сертификат |
| | ни одна сторона, помимо центра сертификации, не может изменить сертификат так, чтобы это не было обнаружено |
| | любой пользователь системы может изменить сертификат |
| | каждый пользователь центра сертификации, имеющий доступ к открытому ключу центра, может изменить открытый ключ, включенный в сертификат |
| Что общего имеют все методы шифрования с закрытым ключом? | в них для шифрования информации используется один ключ, а для расшифрования – другой ключ |
| | в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов |
| | в них производится сложение символов исходного текста и ключа по модулю, равному числу букв в алфавите |
| | в них для шифрования и расшифрования информации используется один и тот же ключ |
| Какие операции применяются обычно в современных блочных алгоритмах шифрования? | возведение в степень |
| | замена бит по таблице замен |
| | нахождение остатка от деления на большое простое число |
| | перестановка бит |
| | сложение по модулю 2 |
| Симметричные методы шифрования – это методы … | шифрования с открытым ключом |
| | сжатия информации |
| | помехоустойчивого кодирования |
| | шифрования с закрытым ключом |
| Как называется сообщение, получение после преобразования с использованием любого шифра? | имитовставкой |
| | ключом |
| | открытым текстом |
| | закрытым текстом |
| Как называется однозначное | коллизия |

| *Вопрос* | *Варианты ответа* |
|---|---|
| преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины? | хеширование |
| | гаммирование |
| | перестановка |
| | сложение по модулю 2 |
| Как называется функция, которая для строки произвольной длины вычисляет некоторое целое значение или некоторую другую строку фиксированной длины? | криптографическая функция |
| | односторонняя функция |
| | хеш-функция |
| | функция Эйлера |
| | функция гаммирования |
| Какие требования предъявляются к криптографическим хеш-функциям? | хеш-функция должна быть применима к сообщению фиксированного размера |
| | при известном значении хеш-функции H(M)=m должно быть трудно (практически невозможно) найти подходящий прообраз M |
| | при известном сообщении M должно быть трудно найти другое сообщение M’ с таким же значением хеш-функции, как у исходного сообщения |
| | для сообщений одинакового размера хеш-код должен получаться одинаковым |
| Какие требования предъявляются к криптографическим хеш-функциям? | хеш-функция должна быть применима к сообщению фиксированного размера |
| | при известном значении хеш-функции H(M)=m должно быть трудно (практически невозможно) найти подходящий прообраз M |
| | при известном сообщении M должно быть легко найти другое сообщение M’ с таким же значением хеш-функции, как у исходного сообщения |
| | должно быть трудно найти какую-либо пару случайных различных сообщений с одинаковым значением хеш-функции |
| Для каких целей применяется хеш-код в криптографии? | для проверки целостности сообщения |
| | для проверки авторства сообщения |
| | для формирования электронной цифровой подписи |
| | для шифрования сообщений |
| | в качестве ключа при шифровании |

**Вопросы к комплексному заданию ТК2**

1. Что относится к средствам инженерно-технической защиты информации и для чего они предназначены?

2. Какие способы аутентификации пользователей могут применяться в компьютерных системах?

3. В чем заключаются основные недостатки парольной аутентификации и как она может быть усилена?

4. Какие биометрические характеристики пользователей могут применяться для их аутентификации? В чем преимущества подобного способа подтверждения подлинности?

5. Что называют двухфакторной аутентификацией?

6. В чем разница между симметричными и асимметричными криптогра-

фическими системами?

7. В чем разница между потоковыми и блочными шифрами?

8. Что такое электронная цифровая подпись, как она получается и проверяется?

9. Какова роль в системах ЭЦП функций хеширования?

10. Какую роль исполняют удостоверяющие центры? Что такое сертификат открытого ключа?

11. Какие программы относят к разряду вредоносных?

12. Что такое компьютерный вирус?

13. Какие существуют виды компьютерных вирусов?

14. В чем разница между загрузочными и файловыми вирусами?

15. Как происходит заражение и функционирование загрузочных вирусов?

16. Какие типы файлов могут заражаться файловыми вирусами?

17. Как происходит заражение программных файлов?

18. Почему файлы документов могут содержать вирусы?

19. Как обеспечивается автоматическое получение управления макровирусами?

20. В чем заключается профилактика заражения компьютерными вирусами?

21. Криптографические примитивы. Хэш-функция и её применения.

**Для текущего контроля ТК3:**

Проверяемая компетенция:

| Код и наименование компетенции | Код и наименование индикатора |
|---|---|
| ОПК-1. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности | ОПК-1.2. Владеет навыками применения цифровых технологий для решения задач профессиональной деятельности с учетом основных требований информационной безопасности |

Тест

| *Вопрос* | *Варианты ответа* |
|---|---|
| К правовым методам защиты информации относится: | разработка нормативно правовых актов, регламентирующих отношения в информационной сфере |
| | создание и совершенствование системы обеспечения ИБ РФ |
| | разработка, использование и совершенствование средств защиты процессов и программ |
| | разработка программ обеспечения ИБ РФ и определение порядка их финансирования |
| | формирование системы мониторинга показателей и характеристик ИБ РФ |
| Информация, использование которой без согласия субъекта может нанести вред его чести, достоинству, деловой репутации | профессиональная тайна |
| | государственная тайна |
| | персональные данные |
| | коммерческая тайна |
| | служебная тайна |

| *Вопрос* | *Варианты ответа* |
|---|---|
| В руководящем документе ФСТЭК системы, в которых работает один пользователь, допущенный ко всей обрабатываемой информации уровня государственной тайны, размещенной на носителях одного уровня конфиденциальности – относятся к группе | 1А |
| | 1Г |
| | 2А |
| | 3А |
| | 3Б |
| К правовым методам защиты информации относится | создание и совершенствование системы обеспечения ИБ РФ |
| | разработка, использование и совершенствование средств защиты процессов и программ |
| | внесение изменений и дополнений в законодательство РФ, регулирующие отношения в области обеспечения ИБ |
| | разработка программ обеспечения ИБ РФ и определение порядка их финансирования |
| | формирование системы мониторинга показателей и характеристик ИБ РФ |
| В руководящем документе ФСТЭК системы, в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации уровня государственной тайны, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности – относятся к группе | 3А |
| | 2А |
| | 1А |
| | 3Б |
| | 1Б |
| К организационно-техническим методам защиты информации относится | создание и совершенствование системы обеспечения ИБ РФ |
| | разработка программ обеспечения ИБ РФ и определение порядка их финансирования; 3. формирование системы мониторинга показателей и характеристик ИБ РФ |
| | уточнение статуса иностранных информационных агентств, СМИ и журналистов |
| В руководящем документе ФСТЭК многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности до грифа «Особо важно» включительно, причем | 1Б |
| | 2Б |
| | 3А |
| | 1А |

| *Вопрос* | *Варианты ответа* |
|---|---|
| различные пользователи имеют различные права на доступ к информации – относятся к группе | 1В |
| Защищаемые государством сведения, распространение которых может нанести ущерб РФ | профессиональная тайна |
| | государственная тайна |
| | персональные данные |
| | коммерческая тайна |
| | служебная тайна |
| В руководящем документе ФСТЭК многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности до грифа «Секретно» включительно, причем различные пользователи имеют различные права на доступ к информации – относятся к группе | 1Б |
| | 2Б |
| | 3А |
| | 1А |
| | 1В |
| К экономическим методам защиты информации относится | разработка программ обеспечения ИБ РФ и определение порядка их финансирования |
| | уточнение статуса иностранных информационных агентств, СМИ и журналистов |
| | внесение изменений и дополнений в законодательство РФ, регулирующие отношения в области обеспечения ИБ |
| | формирование системы мониторинга показателей и характеристик ИБ РФ |
| Информация представляющая секрет производства(ноу-хау), это | профессиональная тайна |
| | государственная тайна |
| | персональные данные |
| | коммерческая тайна |
| | служебная тайна |
| В руководящем документе ФСТЭК многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности в том числе Персональные данные, причем различные | 1Б |
| | 1Г |
| | 3А |
| | 1А |

| *Вопрос* | *Варианты ответа* |
|---|---|
| пользователи имеют различные права на доступ к информации – относятся к группе | 1В |
| К сведениям конфиденциального характера, согласно указу президента рф от 6 марта 1997 г., относятся | информация о распространении программ |
| | информация о лицензировании программного обеспечения |
| | информация, размещаемая в газетах, Интернете |
| | персональные данные |
| | личная тайна |
| Отношения, связанные с обработкой персональных данных, регулируются законом… | «Об информации, информационных технологиях» |
| | «О защите информации» |
| | Федеральным законом «О персональных данных» |
| | Федеральным законом «О конфиденциальной информации» |
| | «Об утверждении перечня сведений конфиденциального характера» |
| Действия с персональными данными (согласно закону), включая сбор, систематизацию, накопление, хранение, использование, распространение и т. д это: | исправление персональных данных |
| | работа с персональными данными |
| | преобразование персональных данных |
| | обработка персональных данных |
| | изменение персональных данных |
| Действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных | выделение персональных данных |
| | обеспечение безопасности персональных данных |
| | деаутентификация |
| | деавторизация |
| | деперсонификация |
| Персональные данные это | любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу |
| | фамилия, имя, отчество физического лица |
| | год, месяц, дата и место рождения, адрес физического лица |
| | адрес проживания физического лица |
| | сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна» |
| Федеральный закон «Об информации, информатизации и защите информации» направлен на: | регулирование взаимоотношений в информационной сфере совместно с гражданским кодексом РФ |
| | регулирование взаимоотношений в гражданском обществе РФ |
| | регулирование требований к работникам служб, работающих с информаций |
| | формирование необходимых норм и правил работы с информацией |
| | формирование необходимых норм и правил, связанных с защитой детей от информации |
| Персональными данными владеют: | государство |
| | различные учреждения |
| | государственная Дума |

| *Вопрос* | *Варианты ответа* |
|---|---|
| | жители Российской Федерации |
| | медико-социальные организации |
| Федеральный закон "Об информации, информатизации и защите информации" дает определение информации: | текст книги или письма |
| | сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления |
| | сведения о явлениях и процессах |
| | факты и идеи в формализованном виде |
| | шифрованный текст, текст на неизвестном языке |
| Укажите нормативно-правовой акт, в котором раскрывается понятие «информационная безопасность» | Закон Российской Федерации от 27 декабря 1991г. №1224-11 «О средствах массовой информации» |
| | Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» |
| | доктрина информационной безопасности |
| | все ответы верны |
| Закон российской федерации «О государственной тайне» был принят в следующем году | 1982 |
| | 1985 |
| | 1988 |
| | 1993 |
| | 2005 |
| Выберите, можно ли в служебных целях использовать электронный адрес (почтовый ящик), зарегистрированный на общедоступном почтовом сервере, например на mail.ru | нет, не при каких обстоятельствах |
| | нет, но для отправки срочных и особо важных писем можно |
| | можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера |
| | можно, если информацию предварительно заархивировать с помощью программы winrar с паролем |
| | можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно |
| Может ли сотрудник быть привлечен к уголовной ответственности за нарушения правил информационной безопасности предприятия | нет, только к административной ответственности |
| | нет, если это государственное предприятие |
| | да |
| | да, но только в случае, если действия сотрудника нанесли непоправимый вред |
| | да, но только в случае осознанных неправомочных действий сотрудника |
| В данном случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности: | выход в Интернет без разрешения администратора |
| | при установке компьютерных игр |
| | в случаях установки нелицензионного ПО |
| | в случае не выхода из информационной системы |
| | в любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности |
| За правонарушения в сфере информации, информационных технологий и защиты | дисциплинарные взыскания |
| | административный штраф |
| | уголовная ответственность |
| | лишение свободы |

| *Вопрос* | *Варианты ответа* |
|---|---|
| информации данный вид наказания на сегодняшний день не предусмотрен: | смертная казнь |
| Информацией, составляющей коммерческую тайну, владеют | государство |
| | различные учреждения |
| | государственная Дума |
| | граждане Российской Федерации |
| | медико-социальные организации |
| Информацией, составляющей государственную тайну, владеют: | государство |
| | только образовательные учреждения |
| | только президиум Верховного Совета РФ |
| | граждане Российской Федерации |
| | только министерство здравоохранения |
| Владельцем информации первой категории является… | государство |
| | коммерческая организация |
| | муниципальное учреждение |
| | любой гражданин |
| | группа лиц, имеющих общее дело |
| Владельцем информации второй категории является… | простые люди |
| | государство |
| | коммерческая организация |
| | муниципальное учреждение |
| | некоммерческая организация |
| Владельцем информации третьей категории является… | люди |
| | государство |
| | муниципальное учреждение |
| | учреждение |
| | некоммерческая организация |
| Основным нормативно-правовым документом, защищающим права, свободы и безопасность человека в системе информационных отношений, в РФ является | Стратегия национальной безопасности РФ |
| | ФЗ "О государственной тайне" |
| | *к*онституция |
| | уголовный кодекс |
| | доктрина информационной безопасности РФ |
| Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ представлены | в *Д*октрине информационной безопасности РФ |
| | в Концепции национальной безопасности РФ |
| | в Конституции РФ |
| | в Билле о надзоре за данными |
| | в ФЗ РФ "Об информации, информационных технологиях и о защите информации" |
| На международном уровне пределы вмешательства в частную жизнь со стороны государства и других субъектов определены | законом о тайне частной информации |
| | стандартом ISO 15408 |
| | оранжевой книгой |
| | *д*екларацией прав человека |
| | биллем о надзоре за данными |

| *Вопрос* | *Варианты ответа* |
|---|---|
| Преступлениям в сфере компьютерной информации в Уголовном кодексе посвящается | *г*лава |
| | раздел |
| | статья |
| | пункт |
| | часть |
| Становление отечественного законодательства по информатизации произошло | в конце 60-х гг |
| | в конце 70-х гг |
| | в конце 80-х гг |
| | в начале 90-х гг |
| | в начале 70-х гг |
| Защита компьютерной информации введена… | семейным кодексом РФ |
| | Конституцией РФ |
| | Гражданским кодексом РФ |
| | Уголовным кодексом РФ |
| Что представляет собой доктрина информационной безопасности РФ? | нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности |
| | федеральный закон, регулирующий правоотношения в области информационной безопасности |
| | целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов |
| | совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации |
| Охрана персональных данных, государственной, служебной и других видов информации ограниченного доступа это | защита информации |
| | компьютерная безопасность |
| | защищенность информации |
| | защищенность потребителей информации |
| | безопасность данных |
| Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ | государственная тайна |
| | коммерческая тайна |
| | банковская тайна |
| | конфиденциальная информация |
| Соотнесите принципы информационной безопасности, определенные Гостехкомиссией | 1. принцип системности |
| | 2. принцип комплексности |
| | 3. принцип непрерывности защиты |
| | 4. гибкость системы защиты |
| | 5. разумная достаточность |
| | 1. правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможно го ущерба были бы приемлемыми |
| | 2. непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС |
| | 3. предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов |
| | 4. освобождает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые |

| *Вопрос* | *Варианты ответа* |
|---|---|
| | 5. предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов |
| Содержание и структура законодательства в области информационной безопасности включает | Конституция Российской Федерации - Нормативно-правовые акты (Указы) Президента Российской Федерации - Подзаконные акты Правительства Российской Федерации - Федеральные законы - Кодексы |
| | Конституция Российской Федерации - Нормативно-правовые акты (Указы) Президента Российской Федерации |
| | Подзаконные акты Правительства Российской Федерации - Федеральные законы - Кодексы |
| | нет верного ответа |
| Законодательство Российской Федерации об информации, информационных технологиях и о защите информации состоит из | федерального закона «Об информации, информационных технологиях и о защите информации» и других федеральных законов, регулирующих отношения в области использования информации |
| | федерального закона «О персональных данных» и других федеральных законов, регулирующих отношения в области использования информации |
| | федерального закона «О коммерческой тайне» и других федеральных законов, регулирующих отношения в области использования информации |
| | федерального закона «О государственной тайне» и других федеральных законов, регулирующих отношения в области использования информации |
| Предметом правового регулирования в области информации, информационных технологий и защиты информации являются | отношения, возникающие только при осуществлении права на поиск, получение, передачу, производство и распространение информации |
| | отношения, возникающие только при применении информационных технологий |
| | отношения, возникающие только при обеспечении защиты информации |
| | отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; при применении информационных технологий; при обеспечении защиты информации |
| В структуру государственной системы защиты информации РФ входят | ФСБ РФ |
| | МВД РФ |
| | ФСТЭК |
| | ФСИН |
| Нормативно-правовой акт - это | правовой акт, принятый полномочным на то органом и содержащий правовые нормы, т. е. предписания общего характера и постоянного действия, рассчитанные на многократное применение |
| | правовой акт, принятый полномочным на то органом и содержащий правовые нормы, т. е. предписания общего характера и постоянного действия, рассчитанные на однократное применение |
| | нет верного ответа |
| Как называется закон, регулирующий деятельность го- | О коммерческой тайне |
| | О государственной тайне |

| *Вопрос* | *Варианты ответа* |
|---|---|
| сударственной тайны на территории РФ | О служебной тайне |
| | О врачебной тайне |
| Субъект персональных данных обладает правами | на доступ к своим персональным данным |
| | возражение против принятия решений исключительно на основании автоматизированной обработки персоналом данных, порождающих юридические последствия в отношении субъекта или иным образом затрагивающих его права и законные интересы |
| | обжалование действий или бездействий |
| | верны все варианты |
| Правовое регулирование отношений в области использования электронной цифровой подписи осуществляется в соответствии с | Гражданским кодексом Российской Федерации |
| | Федеральным законом "Об информации, информатизации и защите информации" |
| | Федеральным законом "О связи" |
| | верны все варианты |
| Что из перечисленного не входит в первый уровень правового обеспечения информационной безопасности | Конституция РФ (ст. 23, право на тайну переписки) |
| | Гражданский кодекс РФ (ст. 139, возмещение убытков от утечек) |
| | Федеральный закон "О государственной тайне" |
| | Постановления Правительства РФ |
| Из скольких уровней состоит правовое обеспечение информационной безопасности | двух уровней |
| | трех уровней |
| | четырех уровней |
| | пяти уровней |
| Перечень видов деятельности в области зашиты информации, на которые выдаются лицензии, определен Постановлением Правительства РФ "О лицензировании отдельных видов деятельности" от 24.12.94 №1418 к ним, в частности, относится разработка, производство, реализация и сервисное обслуживание | шифровальных средств |
| | защищенных систем телекоммуникаций |
| | программных средств |
| | специальных технических средств зашиты информации |
| | подготовка и переподготовка кадров |
| | все верны варианты |
| Законодательной и нормативной базой лицензирования и сертификации в области зашиты информации являются законы РФ | о государственной тайне |
| | о техническом регулировании |
| | о лицензировании отдельных видов деятельности |
| | о защите прав потребителей |
| | все верны варианты |
| Перечень видов деятельности в области зашиты информации, на которые выдаются лицензии, определен Постановлением Правительства РФ "О лицензировании отдель- | шифровальных средств |
| | защищенных систем телекоммуникаций |
| | программных средств |

| *Вопрос* | *Варианты ответа* |
|---|---|
| ных видов деятельности" к ним, в частности, относится разработка, производство, реализация и сервисное обслуживание | специальных технических средств зашиты информации |
| | верны все варианты |
| Какие категории персональных данных выделяет ФЗ “О персональных данных”? | личные |
| | общедоступные |
| | физиологические |
| | специальные |
| | биометрические |
| В каких случаях оператор не обязан уведомлять регулятора об обработке персональных данных? | если данные включают в себя ФИО, телефон и размер оклада |
| | если оператора связывает с субъектом трудовые отношения |
| | если данные включают в себя только ФИО |
| | если данные касаются здоровья субъекта |
| | если данные касаются семейной жизни субъекта |
| | если данные необходимы для однократного пропуска на территорию оператора |
| Выберите случаи обработки персональных данных, когда оператор не обязан получать письменное согласие субъекта на обработку: | бронирование гостиницы туристической фирмой |
| | передача данных третьим лицам |
| | если между оператором и субъектом есть договор, предусматривающий обработку ПД |
| | доставка почтовых сообщений |
| | организация составляет базу данных своих клиентов, с указанием ФИО, телефонов, адресов и занимаемых должностей |
| Какой документ содержит в себе стратегические национальные приоритеты, цели и меры в области внутренней и внешней политики России, определяющие состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу? | Федеральный закон “Об информации, информационных технологиях и о защите информации” |
| | Федеральный закон “О государственной тайне” |
| | Доктрина информационной безопасности Российской Федерации |
| | Стратегия национальной безопасности Российской Федерации |
| Какой документ отображает официальные взгляды на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ? | Федеральный закон “Об информации, информационных технологиях и о защите информации” |
| | Федеральный закон “О государственной тайне” |
| | Доктрина информационной безопасности Российской Федерации |
| | Стратегия национальной безопасности Российской Федерации |

**Вопросы к комплексному заданию ТК3**

1. Что такое «правовое обеспечение информационной безопасности» и в чем заключается его предмет?

2. Раскройте содержание правового обеспечения безопасности сведений.

3. Раскройте содержание и структуру законодательства в области обеспечения информационной безопасности.

4. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

5. Уровни правового обеспечения информационной безопасности.

6. Место информационной безопасности экономических систем в национальной безопасности страны.

7. Основные принципы обеспечения безопасности.

8. Концепция информационной безопасности.

9. Доктрина информационной безопасности России.

10. Четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

11. Основные задачи обеспечения информационной безопасности. Правовые методы обеспечения информационной безопасности

**Для промежуточной аттестации:**

1. Информационная безопасность человека и общества. Уровни защиты информационных ресурсов.

2. Компьютерные преступления. Основные технологии, использующиеся при совершении компьютерных преступлений.

3. Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна.

4. Основные каналы утечки информации.

5. Методы и средства защиты информации. Содержание способов и средств обеспечения безопасности информации.

6. Криптография. Симметричные криптосистемы.

7. Криптография. Асимметричные криптосистемы.

8. Обзор и классификация методов шифрования информации.

9. Электронно-цифровая подпись.

10. Что относится к средствам инженерно-технической защиты информации и для чего они предназначены?

11. В чем заключаются достоинства и недостатки программных средств защиты информации?

12. Парольная защита.

13. Понятие угрозы. Анализ угроз информационной безопасности. Виды «нарушителей».

14. Политика безопасности. Основные типы политики безопасности.

15. Стандарты информационной безопасности.

16. Правовое обеспечение защиты информации. Нормативные документы.

17. Разрушающие программные воздействия: вирусы и закладки. Антивирусные средства.

18. Психологические аспекты информационной безопасности организации.

19. Настройка политики безопасности операционной системы.

20. Анализ защищенности изолированной программной среды.

21. Исследование систем идентификации.

22. Структура законодательной базы информационной безопасности РФ.

23. Стратегия национальной безопасности. Назначение, основные термины.

24. Доктрина ИБ. Ее назначение.

25. Структура и виды нормативных актов, регулирующих обеспечение

информационной безопасности в Российской Федерации

26. Понятие о Защите информации в РФ (149-ФЗ). Государственное регулирование. Обязанности обладателей информации и операторов информационных систем. Регуляторы.

27. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации