ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Стерлитамакский филиал

Колледж

**Рабочая программа дисциплины**

по дисциплине ***ОП.14 Информационная безопасность***

***Общепрофессиональный цикл (вариативная часть)***

специальность

***09.02.07*** ***Информационные системы и программирование***

код наименование специальности

квалификация

***Специалист по информационным системам***

Год начала подготовки
2023

Разработчик (составитель)
***Игдисамова Р.Р.***
преподаватель

Стерлитамак 2023

**Оглавление**

# 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

## 1.1. Область применения рабочей программы

Рабочая программа дисциплины является частью основной образовательной программы в соответствии с ФГОС для специальности: 09.02.07 Информационные системы и программирование (укрупненная группа специальности 09.00.00 Информатика и вычислительная техника), для обучающихся *очной формы* обучения.

## 1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина ОП.14 Информационная безопасность изучается в общепрофессиональном цикле. Дисциплина реализуется в рамках вариативной части

## 1.3. Цель и планируемые результаты освоения дисциплины:

| Код ОК, ПК | Умения | Знания |
|---|---|---|
| ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам | распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника) | актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности |
| ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности | определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска | номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации |
| ОК 04. Эффективно взаимодействовать и работать в | организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, | психологические основы деятельности коллектива, психологические особенности |

| | | |
|---|---|---|
| коллективе и команде | клиентами в ходе профессиональной деятельности | личности; основы проектной деятельности |
| ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках | применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение | современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности |
| ПК 2.1. Разрабатывать требования к программным модулям на основе анализа проектной и технической документации на предмет взаимодействия компонент. | Анализировать проектную и техническую документацию.<br>Использовать специализированные графические средства построения и анализа архитектуры программных продуктов.<br>Организовывать заданную интеграцию модулей в программные средства на базе имеющейся архитектуры и автоматизации бизнес-процессов.<br>Определять источники и приемники данных.<br>Проводить сравнительный анализ.<br>Выполнять отладку, используя методы и инструменты условной компиляции (классы Debug и Trace).<br>Оценивать размер минимального набора тестов.<br>Разрабатывать тестовые пакеты и тестовые сценарии.<br>Выявлять ошибки в системных компонентах на основе спецификаций. | Модели процесса разработки программного обеспечения.<br>Основные принципы процесса разработки программного обеспечения.<br>Основные подходы к интегрированию программных модулей.<br>Виды и варианты интеграционных решений.<br>Современные технологии и инструменты интеграции.<br>Основные протоколы доступа к данным.<br>Методы и способы идентификации сбоев и ошибок при интеграции приложений.<br>Методы отладочных классов.<br>Стандарты качества программной документации.<br>Основы организации инспектирования и верификации.<br>Встроенные и основные специализированные инструменты анализа качества программных продуктов.<br>Графические средства проектирования архитектуры программных продуктов.<br>Методы организации работы в команде разработчиков. |
| ПК 7.4. Осуществлять администрирование баз данных в рамках своей компетенции. | Развертывать, обслуживать и поддерживать работу современных баз данных и серверов. | Модели данных и их типы.<br>Основные операции и ограничения.<br>Уровни качества программной продукции. |
| ПК 7.5. Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации. | Разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных.<br>Владеть технологиями проведения сертификации программного средства | Технология установки и настройки сервера баз данных.<br>Требования к безопасности сервера базы данных.<br>Государственные стандарты и требования к обслуживанию баз данных. |

| | | |
|---|---|---|
| | | |

# 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

## 2.1 Объем дисциплины и виды учебной работы

**Очная форма обучения**

| *Вид учебной работы* | *Объем часов* |
|---|---|
| **Объем образовательной программы** | **110** |
| **Работа обучающихся во взаимодействии с преподавателем** | ***94*** |
| в том числе: | - |
| лекции (уроки) | *32* |
| в форме практической подготовки (если предусмотрено) | * |
| практические занятия | *62* |
| в форме практической подготовки (если предусмотрено) | * |
| лабораторные занятия | - |
| в форме практической подготовки (если предусмотрено) | * |
| курсовая работа (проект) (*если предусмотрена)* | - |
| Самостоятельная работа обучающегося (всего) (*если предусмотрена)* | ***16*** |
| Консультации (*если предусмотрена)* | *4-* |
| Промежуточная аттестация в форме *дифференцированного зачета/зачета/экзамена/итоговой контрольной работы/ курсовой работы* | ***6-*** |

**2.2. Тематический план и содержание дисциплины**

| Наименование разделов и тем | Содержание учебного материала | Объем часов | Осваиваемые элементы компетенций |
|---|---|---|---|
| **1** | **2** | **3** | **4** |
| **Раздел 1. Общие вопросы информационной безопасности.** | | | |
| **Тема 1.1. Международные стандарты информационного обмена** | **Содержание учебного материала** | **4** | ОК 0.1., ОК 0.2., ОК 0.4., ОК 0.9., ПК 2.1. , ПК 7.4., ПК 7.5. |
| | 1. Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации.<br>2. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность з | *4* | |
| | **Практические занятия:** Защита документооборота в вычислительных системах | *10* | |
| **Тема 1.2. Понятия и угрозы** | **Содержание учебного материала** | **4** | ОК 0.1., ОК 0.2., ОК 0.4., ОК 0.9., ПК 2.1. , ПК 7.4., ПК 7.5. |
| | 1.Основные понятия. Механизмы безопасности. Классы безопасности.<br>2.Основные определения и критерии классификации угроз | *4* | |
| | **Практические занятия:** Криптографические методы защиты | *8* | |
| | **Самостоятельная работа обучающихся:**<br>1. Выявление угроз и уязвимостей, каналов утечки информации<br>2. Презентация по теме «Основные угрозы» | *4* | |
| **Раздел 2. Государственная система информационной безопасности** | | | |
| **Тема 2.1 Информационная безопасность в условиях функционирования в России глобальных сетей.** | **Содержание учебного материала** | **4** | ОК 0.1., ОК 0.2., ОК 0.4., ОК 0.9., ПК 2.1. , ПК 7.4., ПК 7.5. |
| | 1. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно справочные документы. Назначение и задачи в сфере обеспечения информационной | *4* | |

| | | | |
|---|---|---|---|
| | безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации<br>2. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны, опасности страны | | |
| | **Практические занятия:** Шифрование методом IDEA | *10* | |
| | **Самостоятельная работа обучающихся:**<br>1. Краткий конспект по теме «Концепция информационной безопасности.»<br>2. Исследовательская работа | *2* | |
| **Раздел 3. Угрозы безопасности** | | | |
| **Тема 3.1. Угрозы безопасности.** | **Содержание учебного материала** | **4** | |
| | 1. Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения.<br>2. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации | 4 | ОК 0.1., ОК 0.2., ОК 0.4., ОК 0.9., ПК 2.1. , ПК 7.4., ПК 7.5. |
| | **Практические занятия:** Шифрование методом RC6 | 10 | |
| | **Самостоятельная работа обучающегося:**<br>1. Виды противников или «нарушителей». Понятие о видах вируса<br>2. 2. Краткий конспект по теме «Причины нарушения целостности информации.» | 2 | |
| **Раздел 4. Теоретические основы методов защиты информационных систем** | | | |
| **Тема 4.1 Теоретические основы методов защиты информационных систем** | **Содержание учебного материала** | **4** | |
| | 1. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности<br>2. 2. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель БеллаЛаПадулы. Ролевая политика | *4* | ОК 0.1., ОК 0.2., ОК 0.4., ОК 0.9., ПК 2.1. , ПК 7.4., ПК 7.5. |

| | | | |
|---|---|---|---|
| | безопасности. Ограничения на области применения формальных моделей | | |
| | **Практические занятия:** Шифрование методом SAFER K-64 | *10* | |
| | **Самостоятельная работа обучающегося:**<br>1. Три вида возможных нарушений информационной системы.<br>2. 2. Доклад по теме «Права доступа Take-Grant» | *2* | |
| **Раздел 5. Методы защиты средств вычислительной техники** | | | |
| **Тема 5.1**<br>**Методы защиты средств вычислительной техники** | **Содержание учебного материала** | **4** | |
| | 1. Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД.<br>2. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности | *4* | ОК 0.1., ОК 0.2., ОК 0.4., ОК 0.9., ПК 2.1. , ПК 7.4., ПК 7.5. |
| | **Самостоятельная работа обучающегося:**<br>1. Виды защиты.<br>2. Выявление угроз и уязвимостей | *2* | |
| **Раздел 6. Основы криптографии** | | | |
| **Тема 6.1**<br>**Основы криптографии** | **Содержание учебного материала** | **4** | |
| | 1. Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи.<br>2. Хеширование. Имитовставки. Криптографические генераторы случайных чисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты. Криптанализ и атаки на криптосистемы | *4* | ОК 0.1., ОК 0.2., ОК 0.4., ОК 0.9., ПК 2.1. , ПК 7.4., ПК 7.5. |
| | **Практические занятия:** Шифрование методом Вернам | *10* | |
| | **Самостоятельная работа обучающегося:**<br>1. Презентация по теме «Криптоанализ»<br>2. Презентация по теме «Электронно-цифровая подпись» | *2* | |
| **Раздел 7. Архитектура защитных экономических систем** | | | |
| **Тема 7.1 Архитектура защитных экономических** | **Содержание учебного материала** | **4** | |
| | 1. Основные технологии построения защищенных | *4* | ОК 0.1., ОК 0.2., ОК 0.4., ОК 0.9., ПК 2.1. , |

| | | | |
|---|---|---|---|
| **систем** | экономических информационных систем. Функции защиты информации. Классы задач защиты информации. Архитектура систем защиты информации.<br>2. Ядро и ресурсы средств защиты информации. Стратегии защиты информации. Особенности экономических информационных систем | | ПК 7.4., ПК 7.5. |
| | **Практические занятия:** Шифрование методом аналитических преобразований | *2* | |
| | **Самостоятельная работа обучающегося:**<br>1. Краткий конспект «Функции защиты информации»<br>2. Доклад на тему «Стратегии защиты информации» | *2* | |
| | **Всего:** | *110* | |

Последовательное тематическое планирование содержания рабочей программы дисциплины, календарные объемы, виды занятий, формы организации самостоятельной работы также конкретизируются в календарно-тематическом плане (Приложение 1)

## 3. ФОРМЫ КОНТРОЛЯ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, ПРАКТИЧЕСКОГО ОПЫТА, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Фонд оценочных средств (далее – ФОС) – комплект методических и контрольных материалов, используемых при проведении текущего контроля освоения результатов обучения и промежуточной аттестации. (Приложение № 2).

## 4. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

### 4.1. Требования к минимальному материально-техническому обеспечению

Для освоения дисциплины требуется учебная аудитория, которая должна удовлетворять требованиям Санитарно-эпидемиологических правил и нормативов и быть оснащена типовым оборудованием, в том числе специализированной учебной мебелью и средствами обучения, достаточными для выполнения требований к уровню подготовки обучающихся

### 4.2. Учебно-методическое и информационное обеспечение дисциплины (модуля)

### 4.2.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

**Основная учебная литература:**

Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927 (дата обращения: 20.09.2020).

Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512861 (дата обращения: 20.09.2020).

**Дополнительная учебная литература:**

Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518005 (дата обращения: 20.09.2020).

Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518006 (дата обращения: 20.09.2020).

### 4.2.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»), необходимых для освоения дисциплины (модуля)

| № | Наименование электронной библиотечной системы |
|---|---|
| 1 | Договор на ЭБС «ЭБС ЮРАЙТ» (полная коллекция) между УУНиТ в лице директора СФ |

| | |
|---|---|
| | УУНиТ и ООО «Электронное издательство ЮРАЙТ» № 5-20 от 04.02.2020 |
| 2 | Договор на ЭБС «Университетская библиотека онлайн» между УУНиТ и «Нексмедиа» № 1132 от 23.09.2020 |
| 3 | Договор на ЭБС между УУНиТ и издательством «Лань» № 1130 от 28.09.2020 |
| 4 | Договор на ЭБС между УУНиТ и издательством «Лань» № 1131 от 28.09.2020 |
| 5 | Договор о подключении к НЭБ и о предоставлении доступа к объектам НЭБ между УУНиТ в лице директора СФ УУНиТ с ФГБУ «РГБ» № 101/НЭБ/1438-П от 11.06.2019 |

| № | Адрес (URL) |
|---|---|
| 1. | http://bookwebmaster.narod.ru/ |
| 2. | http://comp-science.narod.ru |
| 3. | http://www.iXBT.ru |
| 4. | http://sdo.strbsu.ru |

**4.3.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)**

**ПРИЛОЖЕНИЕ 1**

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Стерлитамакский филиал

Колледж

**Календарно-тематический план**

по дисциплине ***ОП.14 Информационная безопасность***

специальность

***09.02.07*** ***Информационные системы и программирование***

код наименование специальности

квалификация

***Специалист по информационным системам***

Разработчик (составитель)

***Игдисамова Р.Р.***

Преподаватель

Стерлитамак 2023

| № п/п | Наименование разделов и тем | Кол-во часов | Календарные сроки изучения (план) | Вид занятия | Домашнее задание |
|---|---|---|---|---|---|
| **Раздел 1. Общие вопросы информационной технологии.** | | | | | |
| 1 | Основные понятия и определения. Понятия информация, | 2/2 | февраль | лекция | Изучить конспект лекции |

| | | | | | |
|---|---|---|---|---|---|
| | информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информаци9онном обмене. Защита информации, тайна, средства защиты информации. | | | | |
| 2 | Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность. | 2/4 | февраль | лекция | Изучить конспект лекции |
| 3 | Основные понятия. Механизмы безопасности. Классы безопасности. | *2/6* | февраль | лекция | Изучить конспект лекции |
| 4 | Основные определения и критерии классификации угроз | *2/2* | февраль | Практическое занятие | выполнение практической работы |
| 5 | Международные стандарты информационного обмена. | *2/4* | март | Практическое занятие | выполнение практической работы |
| 6 | Понятия и угрозы | *2/8* | март | практическое занятие | выполнение практической работы |
| **Раздел 2. Государственная система информационной безопасности.** | | | | | |
| 1 | Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно справочные документы. | *2/8* | март | лекция | Изучить конспект лекции |
| 2 | Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. | *2/10* | март | лекция | Изучить конспект лекции |
| 3 | Доктрина | *2/12* | март | лекция | Изучить |

| | | | | | |
|---|---|---|---|---|---|
| | информационной безопасности Российской Федерации | | | | конспект лекции |
| 4 | Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. | *2/10* | апрель | Практическое занятие | Выполнение практической работы |
| 5 | Структура законодательной базы по вопросам информационной безопасности. | *2/12* | апрель | Практическое занятие | Выполнение практической работы |
| 6 | Лицензирование и сертификация в области защиты информации. | *2/14* | апрель | Практическое занятие | Выполнение практической работы |
| 7 | Место информационной безопасности экономических систем в национальной безопасности страны, опасности страны | *2/16* | апрель | Практическое занятие | Выполнение практической работы |
| **Раздел 3. Угрозы безопасности.** | | | | | |
| 1 | Понятие угрозы. | *2/14* | апрель | лекция | Изучить конспект лекции |
| 2 | Виды противников или «нарушителей». | *2/16* | апрель | лекция | Изучить конспект лекции |
| 3 | Классификация угроз информационной безопасности | *2/18* | апрель | практическое занятие | выполнение практической работы |
| 4 | Виды угроз. Основные нарушения. | *2/20* | май | практическое занятие | выполнение практической работы |
| 5 | Характер происхождения угроз (умышленные и естественные факторы). | *2/22* | май | практическое занятие | выполнение практической работы |
| 6 | Источники угроз. | *2/24* | май | практическое занятие | выполнение практической работы |
| 7 | Предпосылки появления угроз. | *2/28* | май | практическое занятие | выполнение практической работы |
| 8 | Классы каналов несанкционированного получения информации | *2/30* | май | практическое занятие | выполнение практической работы |

| | | | | | |
|---|---|---|---|---|---|
| **Раздел 4. Теоретические основы методов защиты информационных систем.** | | | | | |
| 1 | Основные положения теории информационной безопасности информационных систем. | *2/18* | сентябрь | лекция | Изучить конспект лекции |
| 2 | Модели безопасности и их применение. Формальные модели безопасности | *2/20* | сентябрь | лекция | Изучить конспект лекции |
| 3 | Дискреционная модель Харрисона-Руззо-Ульмана. | *2/32* | сентябрь | Практическое занятие | Выполнение практической работы |
| 4 | Типизированная матрица доступа. | *2/34* | сентябрь | Практическое занятие | выполнение практической работы |
| 5 | Модель распространения прав доступа Take-Grant. Мандатная модель БеллаЛаПадулы | *2/36* | сентябрь | Практическое занятие | выполнение практической работы |
| 6 | Ролевая политика безопасности. Ограничения на области применения формальных моделей | *2/38* | сентябрь | Практическое занятие | выполнение практической работы |
| **Итог** | | **58** | | | |
| **Раздел 5. Методы защиты средств вычислительной техники.** | | | | | |
| 1 | Использование защищенных компьютерных систем. | *2/2* | октябрь | Лекция | Изучить конспект лекции |
| 2 | Аппаратные и программные средства для защиты компьютерных систем от НСД | *2/4* | октябрь | лекция | Изучить конспект лекции |
| 3 | Средства операционной системы. | *2/2* | Октябрь | Практическое занятие | Выполнение практической работы |
| 4 | Средства резервирования данных | *2/4* | Октябрь | Практическое занятие | Выполнение практической работы |
| 5 | Проверка целостности. | *2/6* | Октябрь | Практическое занятие | Выполнение практической работы |
| 6 | Способы и средства восстановления | *2/8* | Ноябрь | Практическое занятие | Выполнение практической работы |
| Раздел 6. Основы криптографии. | | | | | |
| 1 | Методы криптографии. Симметричное и | *2/6* | Ноябрь | лекция | Изучить конспект |

| | | | | | |
|---|---|---|---|---|---|
| | асимметричное шифрование. Алгоритмы шифрования. | | | | лекции. |
| 2 | Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи. | *2/8* | Ноябрь | лекция | Изучить конспект лекции. |
| 3 | Хеширование. | *2/6* | Ноябрь | Практическое занятие | Выполнение практической работы. |
| 4 | Имитовставки. Криптографические генераторы случайных чисел. | *2/8* | Ноябрь | практическое занятие | Выполнение практической работы. |
| 5 | Способы распространения ключей. | *2/10* | Ноябрь | практическое занятие | Выполнение практической работы. |
| 6 | Обеспечиваемая шифром степень защиты. | *2/12* | Ноябрь | практическое занятие | Выполнение практической работы. |
| 7 | Криптанализ и атаки на криптосистемы | *2/14* | ноябрь | практическое занятие | Выполнение практической работы. |
| **Раздел 7. Архитектура защитных экономических систем.** | | | | | |
| 1 | Основные технологии построения защищенных экономических информационных систем. | *2/10* | декабрь | лекция | Изучить конспект лекции. |
| 2 | Функции защиты информации | *2/12* | декабрь | лекция | Изучить конспект лекции. |
| 3 | Классы задач защиты информации. | *2/16* | декабрь | практическое занятие | Выполнение практической работы. |
| 4 | Архитектура систем защиты информации. | *2/18* | декабрь | практическое занятие | Выполнение практической работы. |
| 5 | Ядро и ресурсы средств защиты информации. | *2/20* | декабрь | практическое занятие | Выполнение практической работы. |
| 6 | Стратегии защиты информации. | *2/22* | декабрь | практическое занятие | Выполнение практической работы. |
| 7 | Особенности экономических информационных систем | *2/24* | декабрь | практическое занятие | Выполнение практической работы. |
| **Всего** | | **36** | | | |

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Стерлитамакский филиал

Колледж

**Фонд оценочных средств**

по дисциплине ***ОП.14 Информационная безопасность***

***общепрофессиональный цикл, вариативная часть***
цикл дисциплины и его часть (обязательная, вариативная)

специальность
***09.02.07*** ***Информационные системы и программирование***
код наименование специальности

квалификация
***Специалист по информационным системам***

Разработчик (составитель)
***Игдисамова Р.Р.***
Преподаватель

Стерлитамак 2023

**I Паспорт фондов оценочных средств**

**1. Область применения**

**Фонд оценочных средств** (ФОС) предназначен для проверки результатов освоения дисциплины Информационная безопасность, входящей в состав программы подготовки специалистов среднего звена по специальности 09.02.07 Информационные системы и программирование. **Работа обучающихся во взаимодействии с преподавателем 94 часа**, на самостоятельную работу 16 часов.

**2. Объекты оценивания – результаты освоения дисциплины**

ФОС позволяет оценить следующие результаты освоения дисциплины в соответствии с ФГОС специальности 09.02.07 Информационные системы и программирование и рабочей программой дисциплины Информационная безопасность:

**умения:**

- распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;
- составить план действия; определить необходимые ресурсы;
- владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
- определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска
- организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности
- применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение
- понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
- выявлять достоинства и недостатки коммерческой идеи; презентовать идеи открытия собственного дела в профессиональной деятельности; оформлять бизнес-план; рассчитывать размеры выплат по процентным ставкам кредитования; определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности; презентовать бизнес-идею; определять источники финансирования
- Анализировать проектную и техническую документацию.
- Использовать специализированные графические средства построения и анализа архитектуры программных продуктов.
- Организовывать заданную интеграцию модулей в программные средства на базе имеющейся архитектуры и автоматизации бизнес-процессов.
- Определять источники и приемники данных.
- Проводить сравнительный анализ. Выполнять отладку, используя методы и инструменты условной компиляции (классы Debug и Trace).
- Оценивать размер минимального набора тестов.
- Разрабатывать тестовые пакеты и тестовые сценарии.

- Выявлять ошибки в системных компонентах на основе спецификаций.
- Использовать методы защиты программного обеспечения компьютерных систем.
- Анализировать риски и характеристики качества программного обеспечения.
- Выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами.
- Развертывать, обслуживать и поддерживать работу современных баз данных и серверов.
- Разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных.
- Владеть технологиями проведения сертификации программного средства

**знания:**

- актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте;
- алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
- номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации
- психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности
- современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности
- правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности
- основы предпринимательской деятельности; основы финансовой грамотности; правила разработки бизнес-планов; порядок выстраивания презентации; кредитные банковские продукты
- Модели процесса разработки программного обеспечения.
- Основные принципы процесса разработки программного обеспечения.
- Основные подходы к интегрированию программных модулей.
- Виды и варианты интеграционных решений.
- Современные технологии и инструменты интеграции.
- Основные протоколы доступа к данным.
- Методы и способы идентификации сбоев и ошибок при интеграции приложений.
- Методы отладочных классов.
- Стандарты качества программной документации.
- Основы организации инспектирования и верификации.
- Встроенные и основные специализированные инструменты анализа качества программных продуктов.
- Графические средства проектирования архитектуры программных продуктов.
- Методы организации работы в команде разработчиков.
- Основные средства и методы защиты компьютерных систем программными и аппаратными средствами.
- Модели данных и их типы.
- Основные операции и ограничения.

- Уровни качества программной продукции.
- Технология установки и настройки сервера баз данных.
- Требования к безопасности сервера базы данных.
- Государственные стандарты и требования к обслуживанию баз данных.

Вышеперечисленные умения, знания и *практический опыт* направлены на формирование у обучающихся следующих **общих и профессиональных компетенций**:
способы решения задач профессиональной деятельности, применительно к различным
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 2.1. Разрабатывать требования к программным модулям на основе анализа проектной и технической документации на предмет взаимодействия компонент.
ПК 7.4. Осуществлять администрирование баз данных в рамках своей компетенции.
ПК 7.5. Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации.

**3 Формы контроля и оценки результатов освоения дисциплины**

Контроль и оценка результатов освоения – это выявление, измерение и оценивание знаний, умений и формирующихся общих и профессиональных компетенций в рамках освоения дисциплины.

В соответствии с учебным планом специальности 09.02.07 Информационные системы и программирование, рабочей программой общеобразовательной учебной дисциплины «Информационная безопасность» предусматривается текущий и промежуточный контроль результатов освоения.

**3.1 Формы текущего контроля**

Текущий контроль успеваемости представляет собой проверку усвоения учебного материала, регулярно осуществляемую на протяжении курса обучения.

Текущий контроль результатов освоения дисциплины в соответствии с рабочей программой и календарно-тематическим планом происходит при использовании следующих обязательных форм контроля:

*– выполнение и защита практических работ,*

*- проверка выполнения самостоятельной работы студентов,*

*- проверка выполнения контрольных работ,*

Во время проведения учебных занятий дополнительно используются следующие формы текущего контроля – *устный опрос, решение задач, тестирование по темам отдельных занятий.*

**Выполнение и защита практических работ.** Практические работы проводятся с целью усвоения и закрепления практических умений и знаний, овладения профессиональными компетенциями. В ходе практической работы студенты приобретают умения, предусмотренные рабочей программой дисциплины, учатся *использовать формулы, и применять различные методики расчета, анализировать полученные результаты и делать выводы, опираясь на теоретические знания*.

Список практических работ:

- *Практическая работа №1 «Информация и ее свойства»*
- *Практическая работа №2 «Информационная безопасность»*

**Проверка выполнения самостоятельной работы.** Самостоятельная работа направлена на самостоятельное освоение и закрепление обучающимися практических

умений и знаний, овладение профессиональными компетенциями.

Самостоятельная подготовка обучающихся по дисциплине предполагает следующие виды и формы работы:

- *Систематическая проработка конспектов занятий, учебной и специальной технической литературы.*
- *Самостоятельное изучение материала и конспектирование лекций по учебной и специальной технической литературе.*
- *Написание и защита доклада; подготовка к сообщению или беседе на занятии по заданной преподавателем теме.*
- *Выполнение расчетных заданий.*
- *Работа со справочной литературой и нормативными материалами.*
- *Оформление отчетов по практическим работам, и подготовка к их защите.*
- *Составление тестовых заданий по темам УД/МДК.*

*Выше приводятся формы работы в качестве примера, в зависимости от специфики дисциплины формы и виды самостоятельной работы могут быть отличными.*

**Проверка выполнения контрольных работ.** Контрольная работа проводится с целью контроля усвоенных умений и знаний и последующего анализа типичных ошибок и затруднений обучающихся в конце изучения темы или раздела. Согласно календарно-тематическому плану дисциплины предусмотрено проведение следующих контрольных работ:

- *Контрольная работа №1 по теме «Информация и ее свойства»*
- *Контрольная работа №2 по темам «Информационная безопасность»*

Спецификации контрольных работ приведены ниже в данном комплекте ФОС.

**Сводная таблица по применяемым формам и методам текущего контроля и оценки результатов обучения**

| Результаты обучения | Формы и методы контроля и оценки результатов обучения |
|---|---|
| **Освоенные умения:** | |
| работать с документацией, разработанной с использованием графических языков спецификаций; | Оценка правильности выполнения самостоятельной работы. |
| осуществлять постановку задачи по обработке информации; | Оценка правильности выполнения практических работ. |
| проводить анализ предметной области; | Оценка правильности выполнения практических работ. |
| **Усвоенные знания:** | |
| основные этапы разработки программного обеспечения; | Оценка правильности выполнения практических работ. |
| основные виды работ на этапе сопровождения программного обеспечения; | Оценка правильности выполнения практических работ. |
| основные процессы управления проектом разработки. | Оценка правильности выполнения практических работ. |
| | |

**3.2 Форма промежуточной аттестации**

Промежуточная аттестация по дисциплине Информационная безопасность – *дифференцированный зачет, итоговая контрольная работа*, спецификация которого содержится в данном комплекте ФОС.

*Обучающиеся допускаются к сдаче экзамена при выполнении всех видов самостоятельной работы, практических и контрольных работ, предусмотренных рабочей программой и календарно-тематическим планом дисциплины /МДК.*

*Дифференцированный зачет/зачет/ итоговая контрольная работа проводится за счет времени отведенного на изучение дисциплины/МДК. При условии своевременного и качественного выполнения обучающимся всех видов работ, предусмотренных рабочей программой дисциплины/МДК.*

**Перечень вопросов к дифференцированному зачету**

1. Основные понятия информационной безопасности.
2. Организационно-правовые методы и средства защиты информации.
3. Инженерно-технические методы и средства защиты информации.
4. Программные и программно-аппаратные методы и средства защиты информации.
5. Методы защиты от несанкционированного доступа к информации.
6. Администрирование средств безопасности.
7. Модель политики безопасности.
8. Важность и сложность проблемы информационной безопасности.
9. Основные определения и критерии классификации угроз.
10. Вредоносное программное обеспечение.
11. Основные примитивы криптографии. Подстановки. Перестановки. Гаммирование.
12. Основные примитивы криптографии. Нелинейное преобразование с помощью S-боксов. Комбинированные методы.
13. Основные алгоритмы донаучного периода.
14. Первые криптографические устройства.
15. Алгоритмы симметричного шифрования. Криптография.
16. Сеть Фейштеля.

17. Алгоритмы симметричного шифрования. Криптоанализ.
18. Используемые критерии при разработке алгоритмов симметричного шифрования.
19. Алгоритм DES.
20. Алгоритм ГОСТ 28147.
21. Алгоритм IDEA. Сравнительный анализ с алгоритмом DES.
22. Режимы выполнения алгоритмов симметричного шифрования.
23. Создание случайных чисел.
24. Алгоритмы ассиметричного шифрования. Основные требования к алгоритмам ассиметричного шифрования.
25. Алгоритм RSA.
26. Хэш-функции. Требования к хэш-функциям.
27. Простые хэш-функции.
28. Хэш-функция MD5.
29. Электронная цифровая подпись. Требования к цифровой подписи.
30. Прямая и арбитражная цифровые подписи.
31. Стандарт цифровой подписи DSS.
32. Стандарт цифровой подписи ГОСТ 3410.
33. Криптография с использованием эллиптических кривых. Математические понятия.
34. Аналог алгоритма Диффи-Хеллмана обмена ключами.
35. Алгоритм цифровой подписи на основе эллиптических кривых ECDSA.
36. Шифрование и дешифрование с использованием эллиптических кривых.

**4. Система оценивания комплекта ФОС текущего контроля и промежуточной аттестации**

**Критерии оценивания дифференциального зачета.**

«5» (отлично) – за глубокое и полное овладение содержанием учебного материала, в котором обучающийся свободно и уверенно ориентируется; за умение практически применять теоретические знания, высказывать и обосновывать свои суждения. Оценка «5» (отлично) предполагает грамотное и логичное изложение ответа.

«4» (хорошо) – если обучающийся полно освоил учебный материал, владеет научно-понятийным аппаратом, ориентируется в изученном материале, осознанно применяет теоретические знания на практике, грамотно излагает ответ, но содержание и форма ответа имеют отдельные неточности.

«3» (удовлетворительно) – если обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности в применении теоретических знаний при ответе на практико-ориентированные вопросы; не умеет доказательно обосновать собственные суждения.

«2» (неудовлетворительно) – если обучающийся имеет разрозненные, бессистемные знания, допускает ошибки в определении базовых понятий, искажает их смысл; не может практически применять теоретические знания.

**Критерии оценивания устного опроса.**

«5» (отлично) – за глубокое и полное овладение содержанием учебного материала, в котором обучающийся свободно и уверенно ориентируется; за умение практически применять теоретические знания, высказывать и обосновывать свои суждения; за грамотное и логичное изложение ответа.

«4» (хорошо) – если обучающийся полно освоил учебный материал, владеет научно-понятийным аппаратом, ориентируется в изученном материале, осознанно применяет теоретические знания на практике, грамотно излагает ответ, но содержание и форма ответа имеют отдельные неточности.

«3» (удовлетворительно) – если обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности в применении теоретических знаний при ответе на практико-ориентированные вопросы; не умеет доказательно обосновать собственные суждения.

«2» (неудовлетворительно) – если обучающийся имеет разрозненные, бессистемные знания, допускает ошибки в определении базовых понятий, искажает их смысл; не может практически применять теоретические знания.

**Критерии оценивания контрольной работы.**

Задание к контрольной работе состоит из пяти задач, каждая из которых оценивается в 1 балл.

Решение всех пяти задач соответствует оценке «отлично»,

Решение четырех задач соответствует оценке «хорошо»,

Решение трех задач соответствует оценке «удовлетворительно»,

Решение только двух задач соответствует оценке «неудовлетворительно».

При оценивании *практической и самостоятельной работы* студента учитывается следующее:

- *качество выполнения практической части работы;*
- *качество оформления отчета по работе;*
- *качество устных ответов на контрольные вопросы при защите работы.*

Каждый вид работы оценивается по пяти бальной шкале.

«5» (отлично) – за глубокое и полное овладение содержанием учебного материала, в котором обучающийся свободно и уверенно ориентируется; за умение практически применять теоретические знания, высказывать и обосновывать свои суждения. Оценка «5» (отлично) предполагает грамотное и логичное изложение ответа.

«4» (хорошо) – если обучающийся полно освоил учебный материал, владеет научно-понятийным аппаратом, ориентируется в изученном материале, осознанно применяет теоретические знания на практике, грамотно излагает ответ, но содержание и форма ответа имеют отдельные неточности.

«3» (удовлетворительно) – если обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности, в применении теоретических знаний при ответе на практико-ориентированные вопросы; не умеет доказательно обосновать собственные суждения.

«2» (неудовлетворительно) – если обучающийся имеет разрозненные, бессистемные знания, допускает ошибки в определении базовых понятий, искажает их смысл; не может практически применять теоретические знания.

*Тест оценивается по пяти бальной шкале следующим образом: стоимость каждого вопроса 1 балл. За правильный ответ студент получает 1 балл. За неверный ответ или его отсутствие баллы не начисляются.*

*Оценка «5» соответствует 86% – 100% правильных ответов.*

*Оценка «4» соответствует 73% – 85% правильных ответов.*

*Оценка «3» соответствует 53% – 72% правильных ответов.*

*Оценка «2» соответствует 0% – 52% правильных ответов.*

**Приложение 2**

**Перечень вопросов к устному опросу**

1. Виды компьютерных преступлений.
2. Способы и механизмы совершения информационных компьютерных преступлений.
3. Основные параметры и черты информационной компьютерной преступности в России.
4. Компьютерный вирус. Основные виды компьютерных вирусов.
5. Методы защиты от компьютерных вирусов.
6. Типы антивирусных программ.
7. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
8. Основные угрозы компьютерной безопасности при работе в сети Интернет.
9. Виды защищаемой информации.
10. Государственная тайна как особый вид защищаемой информации.
11. Конфиденциальная информация.

**Перечень заданий к контрольной работе**

1. Информация это -
· сведения, поступающие от СМИ
· только документированные сведения о лицах, предметах, фактах, событиях
· сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
· только сведения, содержащиеся в электронных базах данных

2. Информация
· не исчезает при потреблении
· становится доступной, если она содержится на материальном носителе
· подвергается только "моральному износу"
· характеризуется всеми перечисленными свойствами

3. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется
· достоверной
· конфиденциальной
· документированной
· коммерческой тайной

4. Формы защиты интеллектуальной собственности -
· авторское, патентное право и коммерческая тайна
· интеллектуальное право и смежные права
· коммерческая и государственная тайна
· гражданское и административное право

5. По принадлежности информационные ресурсы подразделяются на
· государственные, коммерческие и личные
· государственные, не государственные и информацию о гражданах
· информацию юридических и физических лиц
· официальные, гражданские и коммерческие

6. К негосударственным относятся информационные ресурсы

· созданные, приобретенные за счет негосударственных учреждений и организаций
· созданные, приобретенные за счет негосударственных предприятий и физических лиц
· полученные в результате дарения юридическими или физическими лицами
· указанные в п.1-3

8. По доступности информация классифицируется на
· открытую информацию и государственную тайну
· конфиденциальную информацию и информацию свободного доступа
· информацию с ограниченным доступом и общедоступную информацию
· виды информации, указанные в остальных пунктах

9. К конфиденциальной информации относятся документы, содержащие
· государственную тайну
· законодательные акты
· "ноу-хау"
· сведения о золотом запасе страны

10. Запрещено относить к информации ограниченного доступа
· информацию о чрезвычайных ситуациях
· информацию о деятельности органов государственной власти
· документы открытых архивов и библиотек
· все, перечисленное в остальных пунктах

11. К конфиденциальной информации не относится
· коммерческая тайна
· персональные данные о гражданах
· государственная тайна
· "ноу-хау"

12. Вопросы информационного обмена регулируются (...) правом
· гражданским3

· информационным
· конституционным
· уголовным

13. Согласно ст.132 ГК РФ интеллектуальная собственность это
· информация, полученная в результате интеллектуальной деятельности индивида
· литературные, художественные и научные произведения
· изобретения, открытия, промышленные образцы и товарные знаки
· исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности

14. Интеллектуальная собственность включает права, относящиеся к
· литературным, художественным и научным произведениям, изобретениям и открытиям
· исполнительской деятельности артиста, звукозаписи, радио- и телепередачам
· промышленным образцам, товарным знакам, знакам обслуживания, фирменным наименованиям и коммерческим обозначениям
· всему, указанному в остальных пунктах

15. Конфиденциальная информация это
· сведения, составляющие государственную тайну
· сведения о состоянии здоровья высших должностных лиц
· документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ
· данные о состоянии преступности в стране

16. Какая информация подлежит защите?
· информация, циркулирующая в системах и сетях связи
· зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать
· только информация, составляющая государственные информационные ресурсы
· любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу

17. Система защиты государственных секретов определяется Законом
· "Об информации, информатизации и защите информации"
· "Об органах ФСБ"
· "О государственной тайне"
· "О безопасности"

18. Государственные информационные ресурсы не могут принадлежать
· физическим лицам
· коммерческим предприятиям
· негосударственным учреждениям
· всем перечисленным субъектам

19. Из нижеперечисленных законодательных актов наибольшей юридической силой в вопросах информационного права обладает
· Указ Президента "Об утверждении перечня сведений, относящихся к государственной тайне"
· ГК РФ
· Закон "Об информации, информатизации и защите информации"
· Конституция

20. Классификация и виды информационных ресурсов определены
· Законом "Об информации, информатизации и защите информации"
· Гражданским кодексом
· Конституцией
· всеми документами, перечисленными в остальных пунктах

21. Определение понятия "конфиденциальная информация" дано в
· 1 ГК РФ
· 2 Законе "О государственной тайне"
· 3 Законе "Об информации, информатизации и защите информации"
· 4 УК РФ

22. Формой правовой защиты литературных, художественных и научных произведений является (...) право
· литературное
· художественное
· авторское
· патентное

23. Запрещено относить к информации с ограниченным доступом
· законодательные акты, информацию о чрезвычайных ситуациях и информацию о деятельности органов государственной власти (кроме государственной тайны)
· только информацию о чрезвычайных ситуациях
· только информацию о деятельности органов государственной власти (кроме государственной тайны)
· документы всех библиотек и архивов

24. Формой правовой защиты изобретений является
· институт коммерческой тайны
· патентное право
· авторское право
· все, перечисленное в остальных пунктах

25. К коммерческой тайне могут быть отнесены
· сведения не являющиеся государственными секретами
· сведения, связанные с производством и технологической информацией
· сведения, связанные с управлением и финансами
· сведения, перечисленные в остальных пунктах

26. Является ли авторское право, патентное право и КТ формами защиты интеллектуальной собственности?
· да
· нет
· только авторское и патентное
· только КТ

27. «Ноу-хау» это -
· незащищенные новшества
· защищенные новшества
· общеизвестные новые технологии
· опубликованные технические и технологические новинки

28. Каким законом в РФ защищаются права исполнителей и производителей фонограмм?
· "О правовой охране программ для ЭВМ и баз данных"
· "Об авторском праве и смежных правах"
· "Патентный закон РФ"
· закон еще не принят

29. Закон "Об авторском праве и смежных правах" защищает права
· исполнителей (актеров, певцов и т.д.)
· производителей фонограмм
· организации эфирного и кабельного вещания
· всех лиц, перечисленных в остальных пунктах

30. Какой законодательный акт содержит сведения по защите коммерческой тайны?
· Закон "Об авторском праве и смежных правах"
· Закон "О коммерческой тайне"
· Патентный закон
· Закон "О правовой охране программ для ЭВМ и баз данных"

31. К информации ограниченного доступа не относится

· государственная тайна
· размер золотого запаса страны
· персональные данные
· коммерческая тайна

32. Система защиты государственных секретов
· основывается на Уголовном Кодексе РФ
· регулируется секретными нормативными документами
· определена Законом РФ "О государственной тайне"
· осуществляется в соответствии с п.1-3

33. Действие Закона "О государственной тайне" распространяется
· на всех граждан и должностных лиц РФ
· только на должностных лиц
· на граждан, которые взяли на себя обязательство выполнять требования законодательства о государственной тайне
· на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения

34. К государственной тайне относится...
· информация в военной области
· информация о внешнеполитической и внешнеэкономической деятельности государства
· информация в области экономики, науки и техники и сведения в области разведывательной и оперативно-розыскной деятельности
· все выше перечисленное

35. Документы, содержащие государственную тайну снабжаются грифом
· "секретно"
· "совершенно секретно"
· "особой важности"
· указанным в п.1-3

36. Гриф "ДСП" используется
· для секретных документов
· для документов, содержащих коммерческую тайну
· как промежуточный для несекретных документов
· в учебных целях

37. Порядок засекречивания состоит в установлении следующих принципов:
· целесообразности и объективности
· необходимости и обязательности
· законности, обоснованности и своевременности
· всех выше перечисленных

38. Предельный срок пересмотра ранее установленных грифов секретности составляет
· 5 лет
· 1 год
· 10 лет
· 15 лет

39. Срок засекречивания сведений, составляющих государственную тайну
· составляет 10 лет
· ограничен 30 годами