Министерство образования и науки Республики (Саха) Якутия

Государственное автономное профессиональное образовательное учреждение

Республики Саха (Якутия)

«Южно-Якутский технологический колледж»

**Рабочая программа**

**МДК.12.03 Специальные технологии выполнения работ по профессии 06.033 Специалист по защите информации в автоматизированных системах по специальности**

**09.02.07 Информационные системы и программирование**

Форма подготовки: очная

г. Нерюнгри, 2020г.

**Аннотация программы**

Рабочая программа МДК.12.03 Специальные технологии выполнения работ по профессии 06.033 Специалист по защите информации в автоматизированных системах разработана в соответствии с федеральным государственным образовательным стандартом, утвержденным приказом Министерства образования и науки Российской Федерации № 1547 от 09.12.2016 г. по специальности среднего профессионального образования **09.02.07 Информационные системы и программирование**, входящей в состав укрупненной группы специальностей **09.00.00 Информатика и вычислительная техника**

Организация-разработчик:

**Государственное автономное профессиональное образовательное учреждение Республики Саха (Якутия) «Южно-Якутский технологический колледж»**

Разработчик:

**Герасимова К.Л., преподаватель ГАПОУ РС(Я) «Южно-Якутский технологический колледж»**

Рецензенты:

**1. Бражник И.Ю., зав. отделением ИТ и СЭС, преподаватель высшей категории ГАПОУ РС(Я) «Южно-Якутский технологический колледж»**

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(дата, подпись)

Рассмотрена и рекомендована предметно – цикловой комиссией «ИТиСД»

Протокол № \_ « \_\_ » \_\_\_\_\_\_ 2023г.

Председатель ПЦК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Саенко В.О./

Рассмотрена и утверждена на заседании отделения Информационных технологий и социально-экономических специальностей

Протокол № \_\_ «\_\_ »\_\_\_\_\_\_\_\_2023г.

Зав.отделением \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Бражник И.Ю. /

**защита информации в автоматизированных системах "**

**СОДЕРЖАНИЕ**

|  |  |  |
| --- | --- | --- |
| 1 | Паспорт программы дисциплины | 4 |
| 1.1. | Область применения программы | 4 |
| 1.2. | Место дисциплины в структуре основной профессиональной образовательной программы | 4 |
| 1.3. | Цели и задачи дисциплины – требования к результатам освоения: | 4 |
| 2 | Структура и содержание дисциплины | 6 |
| 2.1. | Объем дисциплины и виды учебной работы | 6 |
| 2.2. | Тематический план и содержание дисциплины | 8 |
| 2.3. | Обоснование особенностей структурирования содержания | 9 |
| 2.4. | Требования к организации текущей аттестации | 9 |
| 3 | Условия реализации дисциплины | 10 |
| 3.1. | Требования к материально-техническому обеспечению | 10 |
| 3.2. | Информационное обеспечение обучения | 12 |
| 4 | Контроль и оценка результатов освоения дисциплины | 16 |

**1. ПАСПОРТ ПРОГРАММЫ ДИСЦИПЛИНЫ**

**1.1.  Область применения программы**

Рабочая программа дисциплины МДК.12.03 Специальные технологии выполнения работ по профессии: 06.033 Специалист по защите информации в автоматизированных системах является частью образовательной программы подготовки специалистов среднего звена в соответствии с требованиями Федерального государственного образовательного стандарта (далее – ФГОС) утвержденного приказом Министерства образования и науки Российской Федерации № 1553 от 09.12.2016 г. по специальности 09.02.07 Информационные системы и программирование, входящей в состав укрупнённой группы специальностей 09.00.00 Информатика и вычислительная техника

**1.2. Место дисциплины в структуре основной профессиональной образовательной программы**

Дисциплина входит в профессиональный цикл.

**1.3. Цели и задачи дисциплины – требования к результатам освоения:**

В результате освоения дисциплины обучающийся должен **уметь:**

1. устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
2. устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;
3. диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
4. применять программные и программно-аппаратные средства для защиты информации в базах данных;
5. проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;
6. применять математический аппарат для выполнения
7. криптографических преобразований;
8. использовать типовые программные криптографические средства, в том числе электронную подпись;
9. применять средства гарантированного уничтожения информации;
10. устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
11. осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

В результате освоения дисциплины обучающийся должен **знать:**

1. особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
2. методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;
3. типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
4. основные понятия криптографии и типовых криптографических методов и средств защиты информации;
5. особенности и способы применения программных и программноаппаратных средств гарантированного уничтожения информации;
6. типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

В результате освоения дисциплины обучающийся должен **владеть общими и профессиональными компетенциями:**

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности;

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие;

ОК 09. Использовать информационные технологии в профессиональной деятельности.

Перечень профессиональных компетенций, которые формируются в рамках дисциплины

|  |  |
| --- | --- |
| **Код** | **Наименование видов деятельности и профессиональных компетенций** |
| ВД 2 | Защита информации в автоматизированных системах программными и программно-аппаратными средствами |
| ПК 2.1. | Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации |
| ПК 2.2. | Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами |
| ПК 2.3. | Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации |
| ПК 2.4. | Осуществлять обработку, хранение и передачу информации ограниченного доступа |
| ПК 2.5. | Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств |
| ПК 2.6. | Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак |

**2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ**

**2.1 Объем дисциплины и виды учебной работы**

|  |  |
| --- | --- |
| **Вид учебной работы** | **Объем**  **часов** |
| ***7 семестр*** | |
| **Максимальная учебная нагрузка (всего)** | ***62*** |
| **Обязательная аудиторная учебная нагрузка (всего)** | ***60*** |
| лекции | ***20*** |
| практические занятия | ***-*** |
| лабораторная работа | ***40*** |
| консультация | ***-*** |
| **Самостоятельная работа обучающегося** | ***2*** |
| **Промежуточная аттестация в форме** *другие формы* | |
| ***8 семестр*** | |
| **Максимальная учебная нагрузка (всего)** | ***56*** |
| **Обязательная аудиторная учебная нагрузка (всего)** | ***56*** |
| лекции | ***16*** |
| практические занятия | ***-*** |
| лабораторная работа | ***40*** |
| консультация | ***1*** |
| курсовая работа (проект) (*если предусмотрено)* | ***-*** |
| **Промежуточная аттестация в форме** *экзамена* | |

**2.2. Тематический план и содержание**

**МДК.12.03 Специальные технологии выполнения работ по профессии 06.033 Специалист по защите информации в автоматизированных системах по специальности**

**09.02.07 Информационные системы и программирование**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Результаты освоения ОП**  **ОК и ПК** | **Тема** | **Вид учебной нагрузки и часы** | | | | | | | | **Уровень освоения** | **Форма проведения контроля / ФОС приложение** | **Педагогические**  **технологии, методы обучения** |
| **Лекция** | **Практическое**  **занятие** | **Лабораторная работа** | **СРС** | **Курсовая работа (проект)** | **Учебная практика** | **Производственная практика** | **ПДП** |
| **7 семестр** | | | | | | | | | | | | |
| ОК1, ОК2, ОК3, ОК4, ОК5, ОК6, ОК7, ОК8, ОК9, ОК10, ОК11  ПК2.1, ПК2.2, ПК2.3, ПК2.4, ПК2.6. | Предмет и задачи программно-аппаратной защиты информации. | **2** |  |  |  |  |  |  |  | **1** |  |  |
| Основные понятия программно-аппаратной защиты информации | **2** |  |  |  |  |  |  |  | **1** |  |  |
| Анализ терминов и определений информационной безопасности |  |  | **2** |  |  |  |  |  | **2** |  |  |
| Классификация методов и средств программно-аппаратной защиты информации | **2** |  |  |  |  |  |  |  | **1** |  |  |
| Работа с методами программно-аппаратной защиты информации |  |  | **2** |  |  |  |  |  | **2** |  |  |
| Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. | **2** |  |  |  |  |  |  |  | **1** |  |  |
| Работа с ГОСТами в области информационной безопасности |  |  | **2** |  |  |  |  |  | **2** |  |  |
| Обзор нормативных правовых актов, нормативных методических документов по защите информации |  |  | **2** |  |  |  |  |  | **2** |  |  |
| Работа с содержанием нормативных правовых актов |  |  | **2** |  |  |  |  |  | **2** |  |  |
| Обзор стандартов. Работа с содержанием стандартов |  |  | **2** |  |  |  |  |  | **2** |  |  |
| Автоматизация процесса обработки информации. Понятие автоматизированной системы.  Методы создания безопасных систем. Методология проектирования гарантированно защищенных КС | **2** |  |  |  |  |  |  |  | **1** |  |  |
| Уничтожение остаточной информации |  |  | **2** |  |  |  |  |  | **3** |  |  |
| Работа с методами созданиями безопасных систем |  |  | **2** |  |  |  |  |  | **2** |  |  |
| Дискреционные модели. Мандатные модели. | **2** |  |  |  |  |  |  |  | **1** |  |  |
| Учет, обработка, хранение и передача информации в АИС |  |  | **2** |  |  |  |  |  | **2** |  |  |
| Ограничение доступа на вход в систему |  |  | **2** |  |  |  |  |  | **2** |  |  |  |
| Идентификация и аутентификация пользователей |  |  | **2** |  |  |  |  |  | **2** |  |  |  |
| Разграничение доступа. |  |  | **2** |  |  |  |  |  | **2** |  |  |  |
| Регистрация событий (аудит). |  |  | **2** |  |  |  |  |  | **1** |  |  |  |
| Контроль целостности данных |  |  | **2** |  |  |  |  |  | **2** |  |  |  |
| Уничтожение остаточной информации |  |  | **2** |  |  |  |  |  | **2** |  |  |  |
| Управление политикой безопасности. Шаблоны безопасности |  |  | **2** |  |  |  |  |  | **2** |  |  |  |
| Криптографическая защита. Обзор программ шифрования данных |  |  | **2** |  |  |  |  |  | **3** |  |  |  |
| Источники дестабилизирующего воздействия на объекты защиты. Способы воздействия на информацию | **2** |  |  |  |  |  |  |  | **1** |  |  |  |
| Причины и условия дестабилизирующего воздействия на информацию. Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД | **2** |  |  | **1** |  |  |  |  | **2** |  |  |  |
| Распределение каналов в соответствии с источниками воздействия на информацию. |  |  | **2** |  |  |  |  |  | **2** |  |  |  |
| Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Алгоритм загрузки ОС. Расширение BIOS как средство замыкания программной среды | **2** |  |  |  |  |  |  |  | **2** |  |  |  |
| Особенности защиты данных от изменения. | **2** |  |  |  |  |  |  |  | **1** |  |  |  |
| Работа с программой вскрытия паролей AZPR |  |  | **2** |  |  |  |  |  | **2** |  |  |  |
| Организация доступа к файлам |  |  | **2** |  |  |  |  |  | **2** |  |  |  |
| Промежуточный контроль | | Другие формы | | | | | | | | | | |
| **Итого** |  | **20** |  | **40** | **1** |  |  |  |  |  |  |  |
| **8 семестр** | | | | | | | | | | | | |
| ОК1, ОК2, ОК3, ОК4, ОК5, ОК6, ОК7, ОК8, ОК9, ОК10, ОК11  ПК2.1, ПК2.5, ПК2.6. | Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. | **2** |  |  |  |  |  |  |  | **1** |  |  |
| Изучение и обратное проектирование ПО. Способы изучения ПО: статическое и динамическое изучение. Задачи защиты от изучения и способы их решения. Защита от отладки. | **2** |  |  |  |  |  |  |  | **1** |  |  |
| Защита от дизассемблирования. Защита от трассировки по прерываниям. | **2** |  |  |  |  |  |  |  | **1** |  |  |
| Вредоносное программное обеспечение как особый вид разрушающих воздействий. Схема заражения. Средства нейтрализации вредоносного ПО. Основные ветки, содержащие информацию о вредоносном ПО. Поиск следов активности вредоносного ПО. Реестр Windows | **2** |  |  |  |  |  |  |  | **2** |  |  |
| Классификация антивирусных средств. Сигнатурный и эвристический анализ.  Основные концепции построения систем антивирусной защиты на предприятии | **2** |  |  |  |  |  |  |  | **1** |  |  |
| Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО |  |  | **4** |  |  |  |  |  | **3** |  |  |
| Защита информации от несанкционированного копирования с использованием специализированных программных средств |  |  | **4** |  |  |  |  |  | **3** |  |  |
| Защитные механизмы в приложениях |  |  | **2** |  |  |  |  |  | **2** |  |  |
| Проблема защиты отчуждаемых компонентов ПЭВМ |  |  | **2** |  |  |  |  |  | **2** |  |  |
| Средства восстановления остаточной информации. Создание посекторных образов НЖМД. | **2** |  |  |  |  |  |  |  | **1** |  |  |
| Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов |  |  | **4** |  |  |  |  |  | **2** |  |  |
| Безвозвратное удаление данных. Принципы и алгоритмы.  Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ | **2** |  |  |  |  |  |  |  | **1** |  |  |
| Применение средства восстановления остаточной информации на примере Foremost или аналога |  |  | **4** |  |  |  |  |  | **2** |  |  |
| Применение специализированного программного средства для восстановления удаленных файлов |  |  | **4** |  |  |  |  |  | **3** |  |  |
| Применение программ для безвозвратного удаления данных |  |  | **4** |  |  |  |  |  | **3** |  |  |
| Применение программ для шифрования данных на съемных носителях |  |  | **4** |  |  |  |  |  | **2** |  |  |
| Алгоритмы шифрования данных |  |  | **2** |  |  |  |  |  | **2** |  |  |
| Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений |  |  | **2** |  |  |  |  |  | **2** |  |  |
| Защита от копирования. |  |  | **2** |  |  |  |  |  | **2** |  |  |
| Виртуальная частная сеть. Функции, назначение, принцип построения. |  |  | **4** |  |  |  |  |  | **3** |  |  |
| Устройства, образующие VPN.  Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД. Китайская теорема об остатках | **2** |  |  |  |  |  |  |  | **1** |  |  |
| Развертывание VPN |  |  | **2** |  |  |  |  |  | **2** |  |  |
| Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений |  |  | **4** |  |  |  |  |  | **2** |  |  |
| Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида |  |  | **4** |  |  |  |  |  | **2** |  |  |
| Применение Китайской теоремы об остатках в криптосистема RSA |  |  | **4** |  |  |  |  |  | **2** |  |  |
| Промежуточный контроль | | *дифференцированный зачет* | | | | | | | | | | |
| **Итого** |  | **16** |  | **56** |  |  |  |  |  |  |  |  |

1 – ознакомительный (воспроизведение информации, узнавание (распознавание), объяснение ранее изученных объектов, свойств и т.п.);

2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3 – продуктивный (самостоятельное планирование и выполнение деятельности, решение проблемных задач).

**2.3. Обоснование особенностей структурирования содержания**

Программа составлена на основании построения логической структуры содержания данного предмета. Предлагаемый принцип систематизации содержания дает возможность определить время изучения курса, позволяет не только систематизировать содержание по всему учебному курсу, но и дозировать его в процессе обучения.

Структура программы разработана с учетом современных тенденций дифференциации и индивидуализации обучения: предлагается дифференцированное содержание и ориентация на конечный результат (уровня усвоения учебного материала).

**2.4. Требования к организации текущей аттестации**

Ежемесячная аттестация выставляется на основе успешности освоения личностных, метапредметных и предметных результатов:

1. Посещаемость аудиторных занятий за аттестуемый период, не менее 75%;
2. Положительная отметка за выполнение всех практических(лабораторных) работ;
3. Положительная отметка за выполнение всех видов СРС;
4. Промежуточная контрольная работа (при наличии).

Текущая аттестация определяется:

**а** – выполнение требований к ежемесячной аттестации в полном объеме;

**в** – невыполнение в полном объеме требований к ежемесячной аттестации по уважительной причине (при наличии подтверждающих документов);

**с** – невыполнение в полном объеме требований к ежемесячной аттестации по неуважительной причине (отсутствие подтверждающих документов)

**3. условия реализации ПРОГРАММЫ дисциплины**

**3.1 Требования к материально-техническому обеспечению**

Реализация программы дисциплины требует наличия кабинета лаборатории **Технических средств информатизации**

|  |  |  |
| --- | --- | --- |
| Общая номенклатура объектов и средств материально-технического обеспечения для реализации требований ФГОС СПО и содержательным наполнением, учебных дисциплин, междисциплинарных курсов и учебных практик | | **Инвентарные номера (при наличии)** |
| **Наименование объектов и средств** | **Фактическое количество объектов и средств материально-технического обеспечения** |
| **Специализированная учебная мебель** |  |  |
| Стулья | 10 | Б/н |
| Кресла (позволяющие осуществлять поворот сиденья и спинки в пределах ± 1800) | 10 | Б/н |
| Шкафы | 3 | Б/н |
| Стол компьютерный | 12 |  |
| **Технические средства обучения (в том числе экранно-звуковые и цифровые средства)** |  |  |
| Ip-Видеокамера  Коммутатор  Монитор  Моноблок (Розин)  Ноутбук  Презентационный комплекс  Рэк-шкаф  Точка доступа WiFi | 2  14  10  10  12  2  1  1 | 1013400237  1013600238  1013400743  1013400744  1013400745  1013400746  1013400759  1013400768  1013400769  1013400760  1013400761  1013400762  1013400763  1013400764  1013400765  1013400766  1013400704  1013400705  1013400706  1013400707  1013400708  1013400709  1013400710  1013400711  1013400712  1013400713  1013400599  1013400600  1013400601  1013400602  1013400603  1013400604  1013400605  1013400606  1013400607  1013400608  1013400667  1013400676  1013400677  1013400678  1013400679  1013400680  1013400681  1013400682  1013400683  1013400684  1013400668  1013400669  1013400659  1013400660  1013400752  1013400748 |
| Пакеты прикладных программ: текстовых, табличных, графических и презентационных | Комплекс VPN | б/н |
| **Информационно-коммуникативные средства (**лазерные диски, DVD– диски; мультимедийные обучающие, треннинговые, контролирующие и другие программы; электронные учебники и библиотеки; электронные энциклопедии и словари; электронные плакаты, анимационные карто-схемы; инструментальная компьютерная среда для моделирования, программирования и т.п.) |  |  |
| http://real.tepkom.ru/Real\_OM-CM\_A.asp |  | б/н |
| http://programm.ws/index.php |  | б/н |
| http://window.edu.ru/catalog/pdf2txt/699/41699/18857 |  | б/н |
| <http://www.ict.edu.ru> |  | б/н |
| Диполь: Информационная безопасность (Теория, практика, интерактивная коллекция, справочные материалы) |  |  |
| **Перечень сайтов, необходимых для нормативно-правового и учебно-методического обеспечения реализации учебной деятельности** (официальных, образовательных ресурсов, каталогов, методических материалов, периодических изданий в Интернет, из опыта работы, других образовательных организаций и т.п.) |  |  |
| Единое окно доступа к образовательным ресурсамhttp://window.edu.ru/ |  | б/н |
| Российское образование. Федеральный порталhttp://www.edu.ru/ |  | б/н |
| Профообразование http://www.profobrazovanie.org/ |  | б/н |

**3.2. Информационное обеспечение обучения**

**Основные источники:**

1. Бабаш А.В. Криптографические методы защиты информации: учеб. метод. пособия для вузов. Т.1- Т.3 /. — М.: РИОР: ИНФРА-М, 2013. — 413 с.

2. Торстейнсон П. Криптография и безопасность в технологии .NET: Пер. с англ.. - М.: БИНОМ. Лаборатория знаний, 2013. — 479 с.

**Дополнительные источники:**

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации,

информационных технологиях и о защите информации».

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом

регулировании».

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов

деятельности».

5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации

об административных правонарушениях».

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы

Федеральной службы по техническому и экспортному контролю».

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении

перечня сведений конфиденциального характера».

8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по

обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного

обмена».

9. Положение о сертификации средств защиты информации. Утверждено

постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

10. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

11. Меры защиты информации в государственных информационных системах.

Утверждены ФСТЭК России 11 февраля 2014 г.

12. Административный регламент ФСТЭК России по предоставлению государственной

услуги по лицензированию деятельности по технической защите конфиденциальной

информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

13. Административный регламент ФСТЭК России по предоставлению государственной

услуги по лицензированию деятельности по разработке и производству средств защиты

конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г.

№ 84.

14. Специальные требования и рекомендации по технической защите

конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России

от 30 августа 2002 г. № 282.

15. Требования о защите информации, не составляющей государственную тайну,

содержащейся в государственных информационных системах. Утверждены приказом

ФСТЭК России от 11 февраля 2013 г. № 17.

16. Требования о защите информации, содержащейся в информационных системах

общего пользования. Утверждены приказами ФСБ России и ФСТЭК России

от 31 августа 2010 г. № 416/489.

17. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК

России от 6 декабря 2011 г. № 638.

18. Руководящий документ. Геоинформационные системы. Защита информации от

несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК

России, 2008.

19. Руководящий документ. Защита от несанкционированного доступа к информации.

Часть 2. Программное обеспечение базовых систем ввода-вывода персональных

электронно-вычислительных машин. Классификация по уровню контроля отсутствия

недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

20. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г.

№ 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения,

обработки и передачи по каналам связи с использованием средств криптографической

защиты информации с ограниченным доступом, не содержащей сведений, составляющих

государственную тайну».

21. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о

разработке, производстве, реализации и эксплуатации шифровальных (криптографических)

средств защиты информации».

22. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства

обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности

информационных и телекоммуникационных технологий

23. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и

средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности

информационных технологий

24. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и

средства обеспечения безопасности. Часть 4. Выбор защитных мер

25. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и

средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

26. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

27. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства

обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

28. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства

обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

29. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства

обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

30. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита

информации. Процессы формирования и проверки электронной цифровой подписи"

31. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

32. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

33. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

34. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

35. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

38. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

39. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

40. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

41. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

42. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

43. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

44. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

45. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

47. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

48. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

49. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

50. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г. в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники; г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

**Периодические издания:**

1. Журнал о компьютерной технике для профессионалов и опытных пользователей;

Chip/Чип:

2. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/

3. Безопасность информационных технологий. Периодический рецензируемый

научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru

**Электронные источники:**

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

www.fstec.ru

2. Информационно-справочная система по документам в области технической

защиты информации www.fstec.ru

3. Образовательные порталы по различным направлениям образования и тематике

http://depobr.gov35.ru/

4. Справочно-правовая система «Консультант Плюс» www.consultant.ru

5. Справочно-правовая система «Гарант» » www.garant.ru

6. Федеральный портал «Российское образование www.edu.ru

7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/

8. Российский биометрический портал www.biometrics.ru

9. Федеральный портал «Информационно- коммуникационные технологии в

образовании» htpp\\:www.ict.edu.ru

10. Сайт Научной электронной библиотеки www.elibrary.ru

**4. Контроль и оценка** **результатов освоения дисциплины**

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований и других форм.

|  |  |
| --- | --- |
| **Семестр** | **Форма контроля** |
| **7** | Другие формы |
| 8 | Экзамен |

Промежуточной аттестацией по дисциплине является экзамен