МИНИСТЕРСТВО ОБРАЗОВАНИЯ СТАВРОПОЛЬСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
"ПЯТИГОРСКИЙ ТЕХНИКУМ ТОРГОВЛИ ТЕХНОЛОГИЙ И СЕРВИСА"

Комплект
контрольно-оценочных средств

по МДК.03.01 Техническая защита информации

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

2024

1.Паспорт комплекта оценочных средств

1.1 Область применения комплекта оценочных средств

Контрольно-оценочные средства (КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу МДК.03.01 Техническая защита информации.

КОС включают контрольные материалы для проведения промежуточной аттестации в форме экзамена.

КОС разработан на основании рабочей программы МДК.03.01 Техническая защита информации.

1.2. Цели и задачи МДК – требования к результатам освоения МДК

С целью овладения указанным видом деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения МДК должен:

уметь:

У1 применять технические средства для криптографической защиты информации конфиденциального характера;

У2 применять технические средства для уничтожения информации и носителей информации;

У3 применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;

У4 применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;

У5 применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

У6 применять инженерно-технические средства физической защиты объектов информатизации.

знать:

З1 порядок технического обслуживания технических средств защиты информации;

З2 номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;

З3 физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;

З4 порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

З5 методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

З6 номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

З7 основные принципы действия и характеристики технических средств физической защиты;

З8 основные способы физической защиты объектов информатизации;

З9 номенклатуру применяемых средств физической защиты объектов информатизации.

Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции Всероссийского Чемпионата движения по профессиональному мастерству «Профессионалы» по компетенции Корпоративная защита от внутренних угроз информационной безопасности, которые актуализируются при изучении учебной дисциплины:

1) знать и понимать: типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
2) знать и понимать: каналы передачи данных: определение и виды;
3) знать и понимать: технологии работы с политиками информационной безопасности;
4) уметь: создать объекты защиты и политику ИБ, используя технологии анализа в системе корпоративной защиты;
5) уметь: администрирование автоматизированных технические средства управления и контроля информации и информационных потоков;
6) уметь: создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты.

Планируемые личностные результаты освоения рабочей программы

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в

сетевой среде личностно и профессионального конструктивного «цифрового следа»

ЛР 7. Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 9. Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях.

ЛР 10. Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.

ЛР 11. Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.

Результатом освоения МДК является овладение обучающимися видом деятельности - Защита информации техническими средствами, в том числе общие компетенции (ОК) и профессиональными компетенциями (ПК):

Код	**Наименование результата обучения**
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 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению,

	эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

1.3 Результаты освоения междисциплинарного курса, подлежащие проверке

Наименование тем	Коды компетенций (ОК, ПК), личностных результатов (ЛР), умений (У), знаний (З), формированию которых способствует элемент программы	Средства контроля и оценки результатов обучения в рамках текущей аттестации (номер задания)	Средства контроля и оценки результатов обучения в рамках промежуточной аттестации (номер задания/контрольного вопроса/ экзаменационного билета)
Тема 1.1. Предмет и	ОК1	ПЗ №1	ТЗ №1-20

задачи технической защиты информации	З1 ЛР 4 ЛР 10		ПЗ №1-9
Тема 1.2. Общие положения защиты информации техническими средствами	ОК2 З2 З3 ЛР 4 ЛР 7	ПЗ №1	ТЗ №1-20 ПЗ №1-9
Тема 2.1. Информация как предмет защиты	ОК3 ПК 3.2. З2 У3 ЛР 4 ЛР 9 ЛР 10	ПЗ №1	ТЗ №1-20 ПЗ №1-9
Тема 2.2. Технические каналы утечки информации	ОК5 ПК 3.1. З3 У1 ЛР 4 ЛР 9 ЛР 10	ПЗ №2-3	ТЗ №1-20 ПЗ №1-9
Тема 2.3. Методы и средства технической разведки	ОК9 ПК3.2. ПК3.3. З4 З5 У4 ЛР 4 ЛР 9 ЛР 10	ПЗ №4-5	ТЗ №1-20 ПЗ №1-9
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	ОК10 ПК3.2. ПК3.3. З4 З5 У4 ЛР 4	ПЗ №6-7	ТЗ №1-20 ПЗ №1-9
Тема 3.2. Физические процессы при подавлении опасных сигналов	ОК1 ПК3.2. ПК3.3. З7 У4 ЛР 4	ПЗ №8-9	ТЗ №1-20 ПЗ №1-9
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	ОК2 ПК 3.4. З6 У4	ПЗ №10-11	ТЗ №1-20 ПЗ №1-9

	ЛР 4		
Тема 4.2. Системы защиты от утечки информации по проводному каналу	ОК3 ПК 3.4. З8 У6 ЛР 4 ЛР 7	ПЗ №12-13	ТЗ №1-20 ПЗ №1-9
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	ОК5 ПК 3.4. З8 У6 ЛР 4 ЛР 7 ЛР 10	ПЗ №14-15	ТЗ №1-20 ПЗ №1-9
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	ОК5 ПК 3.4. З8 З6 У5 ЛР 10 ЛР 11	ПЗ №16-19	ТЗ №1-20 ПЗ №1-9
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	ОК10 ПК 3.5. У4 З9 ЛР 4 ЛР 10 ЛР 11	ПЗ №20-21	ТЗ №1-20 ПЗ №1-9
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	ОК10 ПК 3.5. З9 У4 ЛР 4 ЛР 10	ПЗ №22-23	ТЗ №1-20 ПЗ №1-9
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	ОК5 ПК 3.5. З8 У6 ЛР 4 ЛР 7 ЛР 9-11	ПЗ №24	ТЗ №1-20 ПЗ №1-9
Тема 5.1. Применение технических средств защиты информации	ОК10 ПК 3.5. У4 З7 ЛР 4 ЛР 7 ЛР 9-11	ПЗ №25-29	ТЗ №1-20 ПЗ №1-9
Тема 5.2.	ОК10	ПЗ №30-33	ТЗ №1-20

Эксплуатация технических средств защиты информации	ПК 3.2. ЛР 4 ЛР 7 ЛР 9-11		ПЗ №1-9

2. Комплект оценочных средств для текущей аттестации

2.1. Практические задания (ПЗ)

ПЗ №1 Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.
ПЗ №2 Основные виду угроз информации
ПЗ №3 Обоснование выбора кабинета как объекта защиты. Составление плана кабинета как объекта защиты
ПЗ №4 Типовая структура технических каналов утечки
ПЗ №5 Моделирование каналов утечки информации. Методы добывания информации о вещественных носителях
ПЗ №6-7 Измерение параметров физических полей
ПЗ №8-9 Защита аппаратуры от электромагнитных полей
ПЗ №10-11 Защита от утечки по акустическому каналу
ПЗ №12-13 Системы защиты от утечки информации по проводному каналу
ПЗ №14-15 Защита от утечки по виброакустическому каналу
ПЗ №16-17 Определение каналов утечки ПЭМИН
ПЗ №18-19 Защита от утечки по цепям электропитания и заземления
ПЗ №20-21 Технические средства защиты информации в телефонных линиях
ПЗ №22-23 Системы защиты от утечки информации по электросетевому каналу
ПЗ №24 Системы защиты от утечки информации по оптическому каналу
ПЗ №25 Применение технических средств защиты
ПЗ №26 Представление моделей объектов информационной безопасности
ПЗ №27 Определение путей проникновения злоумышленника к источнику информации
ПЗ №28 Типовые индикаторы каналов утечки
ПЗ №29 Комплексная система защиты
ПЗ №30 Эксплуатация технических средств защиты
ПЗ №31 Комплексы обнаружения и пеленгации
ПЗ №32 Анализаторы телефонных линий
ПЗ №33 Гарантированное уничтожение информации на магнитных носителях

3. Комплект оценочных средств для промежуточной аттестации

3.1. Тестовые задания (ТЗ)

Задание №1

Создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также

изменение штатных режимов функционирования систем и средств информатизации и связи относится к:

1. правовым методам защиты информации
2. организационно-техническим методам защиты информации
3. организационно-распорядительным методам защиты информации
4. экономическим методам защиты информации

Задание №2

Субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией, называется:

1. собственник информации
2. владелец информации
3. пользователь

Задание №3

Форма допуска, требуемая для работы со сведениями особой важности является:

1. первой формой допуска
2. второй формой допуска
3. третьей формой допуска

Задание №4

Форма допуска, требуемая для работы с совершенно секретными сведениями является:

1. первой формой допуска
2. второй формой допуска
3. третьей формой допуска

Задание №5

Форма допуска, требуемая для работы с секретными сведениями является:

1. первой формой допуска
2. второй формой допуска
3. третьей формой допуска

Задание №6

В сфере государственной тайны действует функционально-зональный принцип. Это значит, что:

1. каждый пользователь допускается должностными лицами только к такой информации, которая требуется ему для исполнения должностных обязанностей
2. каждый пользователь допускается должностными лицами только к информации, касающейся зоны его проживания
3. каждый пользователь допускается должностными лицами ко всей информации, к которой у него есть форма допуска

Задание №7

Противоправные процессы утечки, утраты, распространения, разглашения, копирования, тиражирования, фальсификации, хранения с целью передачи, удаления информации называется процессом:

1. незаконного оборота информации
2. взлома информации
3. несанкционированного использования информации

Задание №8

Форма преднамеренного распространения или мнимого разглашения (утечки) неких планов и намерений, которые не отвечают реальным действиям называется:

1. дезинформация
2. легендирование
3. шпионаж

Задание № 9

Какое направление защиты в основном применяется для охраны материальных ценностей?

1. инженерно-техническая
2. организационно-техническая
3. организационно-распорядительная
4. нормативно-правовая
5. экономическая

Задание №10

Что из нижеперечисленного оборудования может выступать в качестве технического канала связи?

1. контроллер жесткого диска, передающий электрические импульсы, считанные магниторезистивной головкой с поверхности магнитного носителя, по шлейфу в системную магистраль для копирования в оперативную память

2. инфракрасный светодиод лазерного принтера, посылающий кратковременные
3. вспышки на электризованную поверхность фоточувствительного барабана
4. модулированный по силе тока поток электронов, засвечивающий в определенном
5. порядке пикселы люминофора электронно-лучевой трубки
6. экран компьютерного монитора и глаза пользователя
7. оптический канал связи
8. все варианты могут быть отнесены к техническим каналам связи

Задание №11

Какой канал утечки информации основан на использовании электромагнитной энергии видимого и инфракрасного диапазона?

1. визуально-оптический канал
2. электромагнитный канал
3. виброакустический канал
4. материально-вещественный канал

Задание № 12

Процесс перехвата и фиксации процесса клавиатурного ввода идентифицирующей информации является примером утечки информации:

1. визуально-оптического канала
2. электромагнитного канала
3. виброакустического канала
4. материально-вещественного канала

Задание №13

Какой канал утечки информации включает в себя весь радиодиапазон от сверхнизких до сверхвысокочастотных волн?

1. визуально-оптический канал
2. электромагнитный канал
3. виброакустический канал
4. материально-вещественный канал

Задание №14

Электрические сигналы (напряжения, токи), модулированные по закону передаваемого сообщения, протекающие по проводникам и элементам радиоцепей (линиям связи, антеннам, конденсаторам) и возбуждающие в окружающем пространстве электромагнитную энергию является примером утечки информации:

1. визуально-оптического канала
2. электромагнитного канала
3. виброакустического канала
4. материально-вещественного канала

Задание №16

Какой канал утечки информации представляет собой фактический побочный прием модулированной акустической энергии, распространяющейся в газообразной, жидкой или твердой средах

1. визуально-оптический канал
2. электромагнитный канал
3. виброакустический канал
4. материально-вещественный канал

Задание №17

Примером какого канала утечки информации служит звук голоса человека?

1. визуально-оптического канала
2. электромагнитного канала
3. виброакустического канала
4. материально-вещественного канала

Задание №18

По какому признаку делят на классы средства технической разведки (СТР) ?

1. по дальности канала
2. по форме допуска
3. по мощности
4. по степени финансирования

Задание №19

Портативные устройства для запечатления информации, скрытно проносимые на территорию объекта нарушителем на своем теле относят к …

1. первому классу СРТ
2. второму классу СРТ
3. третьему классу СРТ

Задание №20

Для наблюдения за объектами информатизации из-за пределов их охраняемой или контролируемой территории используются СРТ…

1. первого класса

2. второго класса
3. третьего класса

3.2. Практические задания:

1. Выявить и описать потенциальные каналы утечки информации в помещениях. Указать причины возникновения. Составить модель каналов утечки информации.
2. Для помещений определить основные источники информации и их носители. Классифицируйте и опишите категории помещений.
3. Представлены основные варианты возможной утечки речевой информации из объемов выделенных помещений. Определите группы и виды каналов утечки. Опишите технические средства, с помощью которых может быть осуществлен перехват информации.Опишите возможные каналы утечки информации.
4. Опишите методы и средства технической защиты, которые могут применяться для блокирования угроз, связанных с утечкой информации.
5. Для объекта защиты составьте список потенциальных угроз безопасности.
6. Составьте план защиты объекта с помощью технических средств. Поясните расположение и обоснуйте свой выбор.
7. Для объекта защиты выделите и опишите контролируемы зоны ОТСС.
8. Для помещения (объекта защиты) составить проект технической защиты информации от утечки по акустическому каналу.
9. Для помещения (объекта защиты) составить проект технической защиты информации от утечки по оптическому каналу.

4. Критерии оценивания

«5» «отлично»– студент показывает глубокое и полное овладение содержанием программного материала по МДК, в совершенстве владеет понятийным аппаратом и демонстрирует умение применять теорию на практике, решать различные практические и профессиональные задачи, высказывать и обосновывать свои суждения в форме грамотного, логического ответа (устного или письменного), а также высокий уровень овладение общими и профессиональными компетенциями и демонстрирует готовность к профессиональной деятельности;

«4» «хорошо»– студент в полном объеме освоил программный материал по МДК, владеет понятийным аппаратом, хорошо ориентируется в изучаемом материале, осознанно применяет знания для решения практических и профессиональных задач, грамотно излагает ответ, но

содержание, форма ответа (устного или письменного) имеют отдельные неточности, демонстрирует средний уровень овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«3» «удовлетворительно»– студент обнаруживает знание и понимание основных положений программного материала по МДК, но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических и профессиональных задач, не умеет доказательно обосновать свои суждения, но при этом демонстрирует низкий уровень овладения общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«2» «неудовлетворительно» – студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и неуверенно излагает программный материал по МДК, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

5.Информационное обеспечение

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Технические средства информатизации. Учебник для СПО/ Е. И. Гребенюк, Н. А. Гребенюк М.: ИЦ Академия,2019 – 352 с.
2. Технические средства информатизации: учебник/ Гагарина Л.Г. - М.: ИД Форум, 2023.-256 с.

Дополнительные источники:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.
2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015
3. Новиков В.К. Организационное и правовое обеспечение информационнойбезопасности: В 2-х частях. Часть 2 Организационное

обеспечение информационной безопасности: учеб.пособие. – М.: МИЭТ, 2013 – 172 с.
4. Организационно-правовое обеспечениеИнформационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов,В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017 – 336с
5. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие -Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.
6. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации Академия, - 336 с. – 2012
7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд во: ДМК Пресс, - 2012
8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012 – 416 с.
9. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
10. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
11. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
12. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
13. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
14. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
15. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
16. 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».
17. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
18. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с

постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

19. 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.

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

21. 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.

22. 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.

23. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России

24. от 30 августа 2002 г. № 282.

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

26. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России

27. от 31 августа 2010 г. № 416/489.

28. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

29. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

30. 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.

31. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
32. 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
33. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
34. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
35. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
36. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
37. 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
38. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
39. 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
40. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
41. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
42. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
43. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

44. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
45. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
47. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
48. Номенклатура показателей качества. Ростехрегулирование, 2005.
49. 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.
50. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
51. 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.
52. 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.
53. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
54. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
55. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.

56. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
57. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
58. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.
59. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
60. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
61. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Электронные издания (электронные ресурсы):

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с.
2. https://urait.ru/bcode/456793
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с.
4. https://urait.ru/bcode/449548
5. 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 ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с.
6. https://urait.ru/bcode/451933
7. Интерфейсы периферийных устройств –
a. https://intuit.ru/studies/courses/92/92/lecture/28396
8. О компонентах системного блока — подробно –
a. https://intuit.ru/studies/courses/3685/927/lecture/19564?page=2
9. Портативные компьютеры –

a. https://intuit.ru/studies/courses/13910/1276/lecture/24146

10. Сравнительные характеристики процессоров –
a. https://intuit.ru/studies/courses/15812/478/lecture/21074
11. Технические средства информационных технологий –
a. https://intuit.ru/studies/courses/3481/723/lecture/14240
12. Устройства ввода информации –
a. https://intuit.ru/studies/courses/3460/702/lecture/14158
13. Устройства вывода информации –
a. https://intuit.ru/studies/courses/3460/702/lecture/14157
14. DNS [Электронный ресурс] / Официальный сайт интернет-магазина. – Режим доступа: http://dns-shop.ru, свободный.
15. Razgonu [Электронный ресурс] / Информационный портал об аппаратном обеспечении ПК. – Режим доступа: http://razgonu.ru, свободный.
16. Википедия – свободная энциклопедия [Электронный ресурс] / Сайт международного информационного ресурса «Википедия» – Режим доступа: http://ru.wikipedia.org, свободный.
17. КомпьютерПресс [Электронный ресурс] / Официальный сайт периодического издания. – Режим доступа: http://compress.ru/, свободный.
18. Майкрософт [Электронный ресурс] / Официальный сайт корпорации «Майкрософт». – Режим доступа: http://microsoft.com, свободный.
19. Цифровая образовательная среда СПО PROFобразование:

    - Старостин, А. А. Технические средства автоматизации и управления : учебное пособие для СПО / А. А. Старостин, А. В. Лаптева ; под редакцией Ю. Н. Чеснокова. — 2-е изд. — Саратов, Екатеринбург : Профобразование, Уральский федеральный университет, 2019. — 168 с. — ISBN 978-5-4488-0503-5, 978-5-7996-2842-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/87882 (дата обращения: 31.08.2020). — Режим доступа: для авторизир. пользователей

Электронно-библиотечная система:

IPRBOOKS - http://www.iprbookshop.ru/78574.html