МИНИСТЕРСТВО ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»

Комплект
контрольно-оценочных средств
по практике
ПП. 03 Производственная практика

для специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Алексеевка - 2023

Комплект контрольно-оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Составитель:

Ляшенко А.В., преподаватель ОГАПОУ «Алексеевский колледж»

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 ПП.03 Производственная практика.

КОС включают контрольные материалы для проведения промежуточной аттестации в форме дифференцированного зачета.

КОС разработан на основании рабочей программы ПП.03 Производственная практика.

1.2 Цели и задачи практики – требования к результатам освоения рабочей программы практики:

Практика является обязательным разделом образовательной программы. Она представляет собой вид учебной деятельности в форме практической подготовки, направленной на формирование, закрепление, развитие практических навыков и компетенции в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью.

С целью овладения видом деятельности Защита информации техническими средствами и соответствующими профессиональными компетенциями обучающийся в ходе освоения программы учебной практики должен

иметь практический опыт:

- установки, монтажа и настройки технических средств защиты информации;
- технического обслуживания технических средств защиты информации;
- применения основных типов технических средств защиты информации;
- выявления технических каналов утечки информации;
- участия в мониторинге эффективности технических средств защиты информации;
- диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;
- проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;

− проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;

− установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.

уметь:

− применять технические средства для криптографической защиты информации конфиденциального характера;

− применять технические средства для уничтожения информации и носителей информации;

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

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

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

− применять инженерно-технические средства физической защиты объектов информатизации.

знать:

− порядок технического обслуживания технических средств защиты информации;

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

− 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;

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

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

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

− основные принципы действия и характеристики технических средств физической защиты;

− основные способы физической защиты объектов информатизации;

− номенклатуру применяемых средств физической защиты объектов информатизации.

Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции чемпионатного движения по профессиональному мастерству «Профессионалы» и Чемпионата высоких технологий Корпоративная защита от внутренних угроз информационной безопасности, которые актуализируются при изучении профессионального модуля:

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 рабочей программы практики является сформированность у обучающихся первоначальных практических профессиональных умений в рамках профессионального модуля ПМ.03 Защита информации техническими средствами по основному виду деятельности - Защита информации техническими средствами, в том числе профессиональными компетенциями (ПК):

Код	Наименование результата обучения
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 производственной практики, подлежащие проверке

Наименование тем	Коды компетенций (ОК, ПК), личностных результатов (ЛР), умений (У), знаний (З),	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/

	формированию которых способствует элемент программы		экзаменационного билета)
Раздел 1. Применение и эксплуатация технических средств защиты информации	ОК 1-5 ОК10 ПК 3.1.-3.5. ЛР 4 ЛР 7 ЛР 9-11	ПЗ №1-30	ТЗ №1-53 ПЗ №1-10
Раздел 2. Применение и эксплуатация инженерно-технических средств физической защиты	ОК 1-5 ОК10 ПК 3.1.-3.5. ЛР 4 ЛР 7 ЛР 9-11	ПЗ №31-53	ТЗ №1-53 ПЗ №1-10

2. Комплект оценочных средств для текущей аттестации

2.1. Практические задания (ПЗ)

1. Исследование угроз и методологии оценки уязвимости информации.
2. Оценка информационных рисков.
3. Исследование методов и моделей оценки уязвимости информации.
4. Исследование аналитических моделей для определения базовых показателей уязвимости информации.
5. Участие в проектировании политики безопасности информационного объекта.
6. Проектирование политики безопасности информационного объекта на конкретном примере.
7. Мероприятия по выявлению каналов утечки информации (специальные обследования).
8. Участие в монтаже технических средств защиты информации в телефонных линиях
9. Участие в обслуживании и эксплуатации технических средств защиты информации в телефонных линиях
10. Оценка эффективности защиты речевой информации
11. Инструментально-расчётная оценка защищённости защищаемого помещения от утечки речевой информации
12. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности: датчики движения для охраны помещений
13. Участие в монтаже, обслуживании и эксплуатации средств инженерной защиты и технической охраны
14. объектов: системы защиты от утечки информации по оптическому каналу
15. Проектирование системы видеонаблюдения за протяженным периметром.

Проектирование системы

16. идентификации людей на входе в здание. Проектирование системы видеонаблюдения в транспорте.

17. Проектирование системы видеонаблюдения в школе

18. Участие в монтаже систем видеонаблюдения. Участие в обслуживании систем видеонаблюдения.

19. Эксплуатации систем видеонаблюдения. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам: защита информации от утечки по акустическому каналу пассивными методами

20. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам: системы защиты от утечки информации по электросетевому каналу.

3. Комплект оценочных средств для промежуточной аттестации

3.1. Тестовые задания (ТЗ)

1. Инженерно-техническая защита информации. Задачи государственной системы защиты информации защиты
2. Структура государственной системы защиты информации. Направления работ по защите информации.
3. Органы государственной системы защиты информации
4. Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности ее защиты.
5. Понятие о демаскирующих признаках объектов защиты.
6. Характеристики и особенности семантической (смысловой) информации и информации о демаскирующих признаках объекта
7. Классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности объектов.
8. Видовые, сигнальные и вещественные демаскирующие признаки.
9. Основные видовые демаскирующие признаки объектов наблюдения. Особенности видовых признаков в оптическом и радиодиапазона.
10. Определение основных характеристик аналоговых и дискретных (импульсных) электрических сигналов, средств связи, радиолокационных станций, лазерных и других излучений.
11. Изучение основных признаков, характеризующие физические и химические свойства материальных тел. Понятие о демаскирующих объектах, сигналах и веществах.
12. Технические каналы утечки информации.
13. Понятие об опасных сигналах и их источниках.
14. Диагностика основных и вспомогательных технических средств и систем
15. Побочные электромагнитные излучения и наводки.
16. Акустоэлектрические преобразователи, их виды и принципы работы.
17. Принципы высокочастотного навязывания. Высокочастотные и низкочастотные побочные излучения технических средств и систем (ТСС).
18. Паразитная генерация усилителей. Виды паразитных связей между цепями ТСС.
19. Исследование паразитных наводок в цепях электропитания, заземления, в токопроводящих конструкциях помещений и зданий
20. Характеристики каналов утечки информации.

21. Структура технических каналов утечки информации.
22. Виды технических каналов утечки информации.
23. Основные характеристики технических каналов утечки информации.
24. Способы комплексного использования злоумышленниками технических каналов утечки информации
25. Оптические каналы утечки информации. Структура оптического канала утечки информации.
26. Характеристики среды распространения оптических лучей. Основные показатели оптоэлектронных линий связи и способы снятия с них информации.
27. Радиоэлектронные каналы утечки информации. Особенности радиоэлектронных каналов утечки информации. Виды и структура радиоэлектронных каналов утечки информации.
28. Особенности распространения радиоволн различных диапазонов частот. Способы повышения дальности передачи информации в ультракоротком диапазоне радиоволн.
29. Классификация и характеристики помех в радиоэлектронных каналах утечки информации
30. Диагностика акустических каналов утечки информации.
31. Структура акустического канала утечки информации.
32. Отражение и поглощение акустических волн в среде распространения.
33. Понятие о реверберации и влияние времени реверберации на разборчивость речи.
34. Материально-вещественные каналы утечки информации.
35. Анализ способов утечки демаскирующих веществ в твердом, жидком и газообразном виде.
36. Виды потенциальных угроз безопасности информации. Преднамеренные и случайные воздействия на источники информации
37. Технические каналы утечки речевой информации. Технические каналы утечки информации при передачи ее по каналам связи
38. Электрические каналы утечки информации. Электромагнитные каналы утечки информации
39. Средства нейтрализации угроз и управления физической защитой
40. Средства инженерной защиты. Инженерные конструкции
41. Ограждения территорий, зданий, помещений. Двери, окна, ворота. Металлические сейфы, хранилища. Запирающие устройства
42. Биометрические характеристики человека.
43. Устройства управления и исполнения. Турникеты, шлагбаумы, шлюзовые кабины, блокираторы
44. Направленные микрофоны, виды, сравнение характеристик. Диктофоны и стетоскопы.
45. Пульты централизованной охраны.
46. Радиоканальные системы охраны и оповещения. GSM, Internet оповещение
47. Принципы функционирования средств видеонаблюдения. Определение характеристик используемых камер и объективов.
48. Средства отображения видеоинформации. Средства регистрации, хранения и архивации данных. Освещение
49. Системы охранно-тревожной сигнализации. Система пожарной сигнализации
50. Звукоизоляция и звукопоглощение.
51. Диагностика побочных преобразований акустической волны в электрический сигнал.

52. Средства обнаружения, локализации и подавления радиоизлучающих устройств.

53. Средства контроля проводных систем передачи информации.

3.2. Практические задания (ПЗ)

Содержание	
1	Анализ объектов информатизации предприятий, учреждении. организаций
2	Анализ ресурсов обеспечения инженерно-технической защиты информации
3	Оценка эффективности защиты информации
4	Оформление технической и технологической документации
5	Изучение системы технических средств охраны
6	Анализ потенциальных угроз информации
7	Планирование и проектирование внутренних нормативных документов по введению средств защиты информации в эксплуатацию
8	Изучение технических средств защиты информации
9	Получение представления о потенциальной угрозе информации
10	Разработка технической системы защиты информации
	Оформление раздела отчета производственной практики
	Защита отчета по практике

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/ Гагарина Л.Г. - М.: ИД Форум, 2023.-256 с.

2. Техническая защита информации в объектах информационной инфраструктуры (1-е изд.) учебник Бубнов А.А.,М.: ИЦ Академия, 2019 – 272 с.

Дополнительные источники:

1. Гребенюк Е. И., Гребенюк Н. А. Технические средства информатизации. Учебник для СПО М.: ИЦ Академия,2019 – 352 с

2. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.

3. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015

4. 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.

5. Организационно-правовое обеспечениеИнформационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов,В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017 – 336с

6. 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.
7. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации Академия, - 336 с. – 2012
8. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд во: ДМК Пресс, - 2012
9. 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.
10. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
11. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
12. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
13. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
14. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
15. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
16. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
17. 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».
18. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
19. 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.
20. 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.
21. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
22. 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.
23. 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.
24. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России
25. от 30 августа 2002 г. № 282.
26. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
27. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России
28. от 31 августа 2010 г. № 416/489.
29. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
30. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
31. 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.
32. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
33. 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
34. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
35. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
36. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
37. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
38. 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
39. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
40. 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
41. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
42. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
43. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
44. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
45. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
46. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

47. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
48. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
49. Номенклатура показателей качества. Ростехрегулирование, 2005.
50. 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.
51. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
52. 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.
53. 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.
54. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
55. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
56. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.
57. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
58. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

59. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.
60. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
61. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
62. 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 – https://intuit.ru/studies/courses/92/92/lecture/28396
8. О компонентах системного блока — подробно – https://intuit.ru/studies/courses/3685/927/lecture/19564?page=2
9. Портативные компьютеры – https://intuit.ru/studies/courses/13910/1276/lecture/24146
10. Сравнительные характеристики процессоров – https://intuit.ru/studies/courses/15812/478/lecture/21074
11. Технические средства информационных технологий – https://intuit.ru/studies/courses/3481/723/lecture/14240

12. Устройства ввода информации – https://intuit.ru/studies/courses/3460/702/lecture/14158
13. Устройства вывода информации – https://intuit.ru/studies/courses/3460/702/lecture/14157
14. 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:
IPR BOOKS - http://www.iprbookshop.ru/78574.html

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения ОГАПОУ «Алексеевский колледж» http://moodle.alcollege.ru/