Приложение V.1

к программе СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем

ПРОГРАММА ПРЕДДИПЛОМНОЙ ПРАКТИКИ

2023

РАЗРАБОТЧИК:

Место работы	Занимаемая должность	Инициалы, фамилия
ГБПОУ УКРТБ	Преподаватель	Плотникова В.К.

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Преддипломная (квалификационная) практика является завершающим этапом обучения студентов; проводится в соответствии с ФГОС СПО в части государственных требований к минимуму содержания и уровню подготовки выпускников и составленным на его основе учебным планом специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» после освоения теоретического и практического курсов и сдачи студентами всех видов промежуточной аттестации. Студенты, имеющие академические задолженности, к прохождению преддипломной практики не допускаются.

Целью преддипломной практики является подготовка студентов к итоговой государственной аттестации (ИГА). Обеспечение информационной безопасности автоматизированных систем

Задачами преддипломной практики являются:

- сбор студентами-практикантами материалов для выполнения выпускной квалификационной работы и подготовки к ИГА;
- закрепление и углубление в производственных условиях знаний и умений, полученных студентами при изучении общих профессиональных дисциплин «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности» , «Основы алгоритмизации и программирования», «Электроника и схемотехника», «Инженерная и компьютерная графика», «Технические средства информатизации» «Экономика и управление», «Интеллектуальные информационные системы в информационной безопасности», «Кибербезопасность», «Безопасность жизнедеятельности»;
- закрепление и углубление в производственных условиях знаний и умений, полученных студентами при изучении профессиональных модулей «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении», «Защита информации в автоматизированных системах программными и программно-аппаратными средствами», «Защита информации техническими средствами» и во время прохождения учебных и производственных практик (на основе изучения деятельности конкретного предприятия);
- приобретение студентами навыков организаторской работы и оперативного управления производственным участком при выполнении обязанности дублеров инженерно-технических работников со средним профессиональным образованием;
- ознакомление непосредственно на производстве с передовыми технологиями, организацией труда и экономикой производства;
- развитие профессионального мышления и организаторских способностей в условиях трудового коллектива.

Преддипломная практика по специальности ««Обеспечение информационной безопасности автоматизированных систем» организуется на предприятиях, осуществляющих широкое использование вычислительной техники, программно-аппаратных средств и инженерно-технических методов защиты информации или в учебном заведении. Руководителями преддипломной практики назначаются преподаватели специальных дисциплин или высококвалифицированные специалисты.

Бюджет времени, отводимый на преддипломную практику, определяется учебным планом специальности в соответствии с требованиями ГОС СПО.

Для организации преддипломной практики необходимо сформировать пакет документов, включающий рабочую программу производственной практики, график прохождения практики, договора с предприятиями, приказы о распределении студентов по объектам практики.

Объектами профессиональной деятельности студентов в период практики на предприятии являются программно-аппаратные средства и инженерно-технические методы обеспечения информационной безопасности телекоммуникационных систем. Студенты осуществляют сбор материалов для выполнения выпускной квалификационной работы согласно тематическому плану программы практики.

Предприятия, являющиеся базами практики студентами, должны соответствовать современным требованиям и перспективам развития технических средств защиты информации, информационных систем и вычислительной техники, оснащены высокопроизводительным оборудованием, прогрессивными технологиями, иметь в наличии квалифицированный персонал.

Итогом преддипломной практики является оценка, которая приравнивается к оценкам теоретического обучения и учитывается при подведении результатов общей успеваемости студентов. Оценка выставляется руководителем практики от колледжа на основании собеседования со студентом и его отчета о прохождении практики, с учетом личных наблюдений за самостоятельной работой практиканта, характеристики и предварительной оценки руководителя практики от предприятия.

Студенты, не выполнившие требований программы преддипломной практики или получившие отрицательную характеристику, отчисляются из колледжа.

ПРИМЕРНЫЙ ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Наименование видов, разделов и тем практики	Количество часов (недель)
1.	Вводное занятие. Ознакомление с предприятием. Инструктаж по технике безопасности.	0.2
2.	Практика на рабочих местах.	3.6
2.1	Обоснование актуальности темы выпускной квалификационной работы	1.0
2.2	Постановка проблемы, анализ степени исследованности проблемы, обзор литературы	1.3
2.3	Содержательная характеристика объекта исследования	1.3
3.	Оформление отчета. Зачет по преддипломной практике.	0.2
Всего		4

ПРИМЕРНОЕ СОДЕРЖАНИЕ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Темы, учебная информация, необходимая для овладения умениями и навыками	Формируемые умения и навыки	Примерные виды работ	Связь с учебными дисциплинами
1	2	3	4
1.Вводное занятие и инструктаж по технике безопасности. Задачи и краткое содержание практики по профилю специальности. Инструктаж по общим вопросам, охраны труда и техники безопасности, по режиму работы предприятия. Изучение структуры предприятия и взаимосвязи подразделений. Основная деятельность предприятия. Изучение политики информационной безопасности предприятия	Организация рабочего места и мероприятий по обеспечению безопасности.		Безопасность жизнедеятельности. Правовое обеспечение профессиональной деятельности. Экономика, Основы информационной безопасности
2.Практика на рабочих местах. 2.1 Обоснование актуальности темы выпускной квалификационной работы.	Обладание широким кругозором Способность к осмыслению жизненных явлений. Анализ и синтез информации.	Работа с технической и справочной литературой и Internet.	Общие профессиональные дисциплины и профессиональные модули.
2.2 Постановка проблемы, анализ степени исследованности проблемы, обзор литературы.	Комплексное представление об основных аспектах развития систем информационной безопасности в организациях различных структур.	Изучение проблем и перспектив развития средств обеспечения информационной безопасности.	Общие профессиональные дисциплины и профессиональные модули.

2.3 Содержательная характеристика объекта исследования.	Владение информацией о назначении и функционировании создаваемого продукта технического творчества	Описание создаваемого продукта технического творчества	Общие профессиональные дисциплины и профессиональные модули
3.Оформление отчета. Зачет по преддипломной практике.	Оформление документации в соответствии с действующими нормативными документами	Создание отчета	Общие профессиональные дисциплины и профессиональные модули

ПРИМЕРНАЯ ТЕМАТИКА ВЫПУСКНЫХ КВАЛИФИКАЦИОННЫХ РАБОТ

1. Разработка мессенджера с использованием шифрования Signal Protocol
2. Обеспечение безопасности предприятия с помощью удостоверяющего центра
3. Обеспечение безопасности предприятия с помощью Astra Linux
4. Комплексная система защиты предприятия
5. Внедрение облачного СКУД в ООО НПП БУРИНТЕХ
6. Обеспечение безопасного подключения с помощью OpenVPN
7. Построение комплексной системы защиты от нсд, с использованием модулей доверенной загрузки "Соболь"
8. Разработка системы защиты помещения с применением звукомаскирующей системы
9. Построение системы комплексной системы защиты от нсд, с использованием СЗИ SecretNet

ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ОТЧЕТА

По завершению прохождения практики студент должен сформировать и представить руководителю практики от колледжа отчет, содержащий:

1. Титульный лист
2. Договор с предприятием о прохождении практики (в случае прохождения студентом практики в индивидуальном порядке)
3. Характеристику, выданную на предприятии, подписанную руководителем практики от предприятия и заверенную печатью
4. Отчет, представляющий собой введение и общую часть выпускной квалификационной работы.

Отчет должен содержать следующие разделы:

1. Обоснование актуальности темы
2. Постановка проблемы, анализ степени исследованности проблемы, обзор литературы

3. Содержательная характеристика объекта исследования

Отчет по объему должен занимать не менее 12-15 страниц формата А4 и содержать иллюстрации (экранные формы).

Требования к шрифту:

- заголовки выполняются 14 шрифтом (жирным);
- основной текст выполняется 12 или 14 шрифтом (обычным);
- наименования разделов выполняются по центру.

Отчет по преддипломной практике представляется руководителю практики от колледжа не позднее 3-х дней после ее завершения на бумажном (подшитом в папку) и электронном (диске) носителях.

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2021.
2. Милославская Н.Г., Толстой А.И. Управление рисками информационной безопасности. - 3-е изд.- М.: Горячая линия-Телеком, 2022.
3. Мельников Д. Информационная безопасность открытых систем.- М.: Форум, 2019.
4. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание – Питер, 2020.
5. Батаев А.В., Синицын С.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2021.
6. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020.
7. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – Питер, 2022.
8. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А.В. Васильков, И.А. Васильков. — Москва : ФОРУМ : ИНФРА-М, 2020. — 368 с. — (Среднее профессиональное образование). - ISBN 978-5-91134-360-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1082470 (дата обращения: 26.02.2023).
9. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2017.- 175 с.
10. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с.
11. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с.
12. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.
13. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

14. 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.

15. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учебное пособие). - М.: Гелиос АРВ, 2005. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности

16. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012

17. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012

18. 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.

19. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2020.

20. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2021.

21. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2019. – 184 с.

22. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб.пособие. – М.: МИЭТ, 2019. – 172 с.

23. Е.Б. Белов, В.Н. Пржегорлинский Организационно-правовое обеспечение информационной безопасности: учеб.пособие для студ. учреждений сред. проф. образова-ния/. – М.: Издательский центр «Академия», 2019. – 336с

24. Ю.Ю. Коваленко. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебное пособие / – М.: Горячая линия – Телеком, 2019.

25. Электронный конспект лекций «Инженерно-техническая защита информации». Составитель: И.Н. Драч, преподаватель ГБОУ СПО РО «РКСИ»

26. Электронный конспект лекций «Криптографическая защита информации». Составитель: Шигаева С.В., преподаватель ГБОУ СПО РО «РКСИ»

27. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2020.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для сту-дентов высших учебных заведений.

28. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2022

29. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012

30. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности: учебник: Рекомендовано УМО, 2019. - 192с.

31. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2022. – 416 с.

32. Информатика: учебник для сред. Проф. Образования/ Е.В. Михеева, О.И. Титова. – М.: Издательский центр « Академия», 2020.

33. Немцова Т.И., Назарова Ю.В. Информатика. практикум по информатике: учеб. Пособие/ Под ред. Л.Г. Гагариной Ч. I. – М.: ИД «ФОРУМ»: ИНФРА-М, 2022

Дополнительные печатные источники:

1. Кумскова И.А. Базы данных. Учебник. СПО. /Издательство «КноРус» 2022. – 400с.

2. Советов Б., Цехановский В., Чертовской В. Базы данных: учебник/ Издатель: Юрайт // 2022 – 421с.

3. Основы проектирования баз данных: учебное пособие / Шитов В.Ш. – Москва: ИНФРА-М, 2023.

4. Нестеров С. А., Базы данных. Учебник и практикум для СПО/ Профессиональное образование /Издатель: ЮРАЙТ,2019.

5. Партыка, Т. Л. Операционные системы, среды и оболочки : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 560 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-501-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189335 (дата обращения: 26.02.2023). – Режим доступа: по подписке.

6. Рудаков, А. В. Операционные системы и среды : учебник / А.В. Рудаков. — Москва : КУРС : ИНФРА-М, 2022. — 304 с. — (Среднее профессиональное образование). - ISBN 978-5-906923-85-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843025 (дата обращения: 26.02.2023).

7. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2022. — 327 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1865598 (дата обращения: 26.02.2023). Программно-аппаратные средства обеспечения информационной безопасности. Практикум : учебное пособие / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов [и др.] ; под. ред. А. В. Душкина. - Москва : Горячая линия-Телеком, 2020. - 412 с. - ISBN 978-5-9912-0797-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1911636 (дата обращения: 26.02.2023).

8. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Учебное пособие.- 2-е изд., испр.- М.: Интернет-Университет ИТ; БИНОМ. Лаборатория знаний, 2020.- 605 с.

9. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 4-е изд. – М.: Вильямс, 2004. – 656 с.

10. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учеб. Пособие для вузов.- 3-е изд., стер. М.: Горячая линия, 2011.- 147 с.

11. . 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, 2019. — 240 с. — (Профессиональное образование). — ISBN 978-5-534-10711- 1. — Текст : электронный // ЭБС Юрайт [сайт].
12. 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, 2019. — 240 с. — (Профессиональное образование). — ISBN 978-5-534-10711- 1. — Текст :электронный // ЭБС Юрайт [сайт]
13. Руководство администратора Криптон-замок
14. Руководство администратора ППКОП «Астра»
15. Руководство администратора КТМ-256
16. Учебное пособие Структурированная кабельная система NIKOMAX»
17. - Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информацион-ных технологиях и о защите информации».
18. - Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
19. - Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
20. - Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
21. - Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
22. - Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
23. - Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
24. - 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».
25. - Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
26. - Положение о сертификации средств защиты информации по требованиям безопас-ности информации (с дополнениями в соответствии с постановлением Правитель-ства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии Рос-сии от 27 октября 1995 г. № 199.
27. - Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.
28. - 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.
29. Практикум по информатике: учеб. пособие для студ. учреждений сред. проф. образования/ Е.В. Михеева.-8-е изд., стер. – М.: Издательский центр «Академия», 2020-192 с.
30. Сборник задач и упражнений по информатике: Учебное пособие/В.Д.Колдаев, под ред. Л.Г.Гагариной - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2019 - 256 с
31. Современные операционные системы. Таненбаум Э. 2022, 4-е изд., 1120с.
32. Технические средства информатизации. Практикум. (для ССУЗов) Лавровская О.Б. 2022, 208с.
33. Установка и обслуживание программного обеспечения персональных компьютеров, серверов, периферийных устройств и оборудования. (СПО) Богомазова Г.Н., 2022, 256с.)

34. Информационные технологии / А. А. Хлебников. – Москва : КНОРУС, 2019 – 472 с. – Бакалавриат.
35. Информационные технологии: Учебник/М.Е. Елочкин, Ю.С. Брановский, И.Д. Николаенко. – М.: Издательство Оникс, 2012.
36. Аппаратное обеспечение ЭВМ. Практикум. (для ССУЗов) Струмпэ Н.В., Сидоров В.Д. 2019, 160с.
37. А. С. Грошев Информатика: лабораторный практикум. –
38. Архангельск, 2020. – 151 с.
39. Оператор ЭВМ. Практические работы: учеб. пособие для НПО/
40. Н.В. Струмпэ. – 5-е изд., стер. – М.: Издательский центр «Академия», 2023. – 112с.

Периодические издания:

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

2. Журналы Защита информации. Инсайд: Информационно-методический журнал

3. Информационная безопасность регионов: Научно-практический журнал

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

5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

Электронные источники:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Российский биометрический портал www.biometrics.ru
5. Сайт журнала Информационная безопасность http://www.itsec.ru –
6. Сайт Научной электронной библиотеки www.elibrary.ru
7. Справочно-правовая система «Гарант» » www.garant.ru
8. Справочно-правовая система «Консультант Плюс» www.consultant.ru
9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
10. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
11. Федеральный портал «Российское образование www.edu.ru
12. 1. 1. Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов. - М.: МЦНМО, 2006. Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2006 г
13. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
14. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
15. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

16. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
17. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
18. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
19. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
20. 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».
21. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
22. 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.
23. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
24. 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.
25. 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.
26. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
27. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
28. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России 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 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».
33. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

34. 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
35. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
36. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
37. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
38. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
39. 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
40. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
41. 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
42. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
43. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
44. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
45. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
46. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
47. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
48. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
49. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
50. Номенклатура показателей качества. Ростехрегулирование, 2005.
51. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.
52. 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.
53. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
54. 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.
55. 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.
56. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
57. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
58. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
59. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
60. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
61. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
62. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
63. 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.

64. . http://www.morion.ru/
65. http://www.nateks.ru/
66. http://www.iskratel.com/
67. http://www.ps-ufa.ru/
68. http://3m.com/
69. http://www.rusgates.ru/index/php - Материалы сайта завода «Ферроприбор»
70. http://cryptogrof.ru/