

Приложение V.1
к программе СПО 10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем

ПРОГРАММА ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Уфа 2019

РАЗРАБОТЧИК:

| | | |
|--------------|----------------------|-------------------------------|
| Место работы | Занимаемая должность | Инициалы, фамилия |
| ГБПОУ УКРТБ | Преподаватель | Хакимова Г.Г. Арефьев А.В. |

СОДЕРЖАНИЕ

стр.

1. Пояснительная записка
2. Примерный тематический план
3. Примерное содержание преддипломной практики
4. Примерная тематика выпускных квалификационных работ
5. Требования к оформлению отчета
6. Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

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 10.02.02 «Информационная безопасность телекоммуникационных 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).

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 «Инженерная графика», «Электротехника», «Электроника и схемотехника», «Электрорадиоизмерения и метрология», «Основы информационной безопасности», «Вычислительная техника», «Основы алгоритмизации и программирования», «Экономика организации», «Менеджмент», «Элементы и узлы периферийных устройств компьютерных систем», «Интегрированные информационно-управляющие компьютерные системы», «Интеллектуальные информационные системы», «Теория принятия решений», «Безопасность жизнедеятельности»;
- закрепление и углубление в производственных условиях знаний и умений, полученных студентами при изучении профессиональных модулей «Техническое обслуживание оборудования защищенных телекоммуникационных систем», «Применение программно-аппаратных, инженерно-технических методов и средств обеспечения информационной безопасности телекоммуникационных систем», «Участие в организации работ по обеспечению информационной безопасности телекоммуникационных систем» 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 «Информационная безопасность телекоммуникационных 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 |
| <p>1. Вводное занятие и инструктаж по технике безопасности.</p> <p>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</p> | <p>Организация рабочего места и мероприятий по обеспечению безопасности.</p> | | <p>Безопасность жизнедеятельности. Правовое обеспечение профессиональной деятельности. Экономика, Основы информационной безопасности</p> |
| <p>2. Практика на рабочих местах.</p> <p>2.1 Обоснование актуальности темы выпускной квалификационной работы.</p> | <p>Обладание широким кругозором. Способность к осмыслению жизненных явлений. Анализ и синтез информации.</p> | <p>Работа с технической справочной литературой и Internet.</p> | <p>Общие профессиональные дисциплины и профессиональные модули.</p> |
| <p>2.2 Постановка проблемы, анализ степени исследованности проблемы, обзор литературы.</p> | <p>Комплексное представление об основных аспектах развития систем информационной безопасности в организациях различных структур.</p> | <p>Изучение проблем и перспектив развития средств обеспечения информационной безопасности.</p> | <p>Общие профессиональные дисциплины и профессиональные модули.</p> |

| | | | |
|---|--|--|---|
| 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 устройства системы защиты на основе алгоритмических шифраторов.
2. Разработка микроконтроллерного устройства управления исполнительными блоками для режимных объектов.
3. Разработка лабораторного стенда для изучения работы средств видеонаблюдения и регистрации.
4. Разработка лабораторного стенда для изучения управления контролем доступа.
5. Разработка учебного стенда биометрической системы контроля управления доступом.
6. Разработка электронных учебно-методических комплексов.
7. Проектирование систем видеонаблюдения.
8. Разработка методического обеспечения для лаборатории УГКР.
9. Построение защиты локальной вычислительной сети предприятия.
10. Разработка комплексной защиты предприятия.
11. Построение защиты информационных систем персональных данных предприятия.

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. Телекоммуникационные системы и сети: Учебное пособие в 3 томах. Том 2 – Радиосвязь, радиовещание, телевидение / Катунин Г.П., Мамчев Г.В., Попантопуло В.Н., В.П. Шувалов; под ред. Профессора В.П. Шувалова. – изд. 2-е и до. – М.: Горячая линия – Телеком, 2015.
2. Садовиковский А.С., Приемо-передающие радиоустройства и системы связи: Учебное пособие для студентов специальности 21020165 / А.С. Кадомовский. – Ульяновск: УлГТУ, 2016.
3. Чернышев Е.И. Линейные сооружения связи: учебное пособие для СПО. – Волгоград: «Ин-Фолио», 2016;
4. Гроднев И.И. Линейные сооружения связи: учебник для техникумов. – М.: Радио и связь, 2015;
5. Парфенов Ю.А. Кабели электросвязи. М.: Эко-Трендз, 2016;
6. Иоргачев Д.В. Бондаренко О.В. Волоконно-оптические кабели и линии связи. – М.: ЭКО_ТРЕНДЗ, 2016;
7. [http://izmer-ls.ru/Руководство по эксплуатации линейно-кабельных сооружений местных сетей связи. \(Утв. ГОСКОМСВЯЗИ РФ 05.06.1998\);](http://izmer-ls.ru/Руководство по эксплуатации линейно-кабельных сооружений местных сетей связи. (Утв. ГОСКОМСВЯЗИ РФ 05.06.1998);)
8. Ксенофонтов С.Н. Портнов Э.Л. Направляющие системы электросвязи. Сборник задач; учебное пособие для ВУЗов. 2-е изд. стереотип, - М.:
9. Хрусталева З.А. Источники питания радиоаппаратуры: учебник для студ. учреждений сред. проф. образования / З.А. Хрусталева, С.В. Парфенов. – М.: Издательский центр «Академия», 2016 – 240 с.
10. Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие/ Фороузан Б.А.; пер. с англ. Под ред. А.Н. Берлина. - М.: Интернет-Университет Информационных технологий: БИНОМ. Лаборатория знаний, 2015.-784с.:ил.,табл.-(Основы информационных технологий). 2. Максименко В.Н., Афанасьев В.В., Волков Н.В. Защита информации в сетях сотовой подвижной связи/ Под ред. доктора техн. Наук, профессора О.Б. Макаревича. – М.: Горячая линия – Телеком, 2016. -360с.: ил.
11. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства –М.: ДМК Пресс, 2015. – 544с.:ил.
12. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. –СПб.:2015.-272с.:ил.
13. Васильков А.В., Васильков А.А., Васильков И.А Информационные системы и их безопасность: учебное пособие –М.: ФОРУМ, 2016.-528с.- (Профессиональное образование)

14. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Техническая защита информации. Учебник для вузов -5-е изд., перераб. и доп. – М.: - Горячая линия – Телеком, 2016. – 616с:ил.
15. Романов О.А. Организационное обеспечение информационной безопасности: учебник для студентов высш. учеб. заведений –М.: Издательский центр «Академия», 2015. – 192с.
16. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2015.
17. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015.
18. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2016. – 184 с.
19. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2016. – 172 с.
20. Е.Б. Белов, В.Н. Пржегорлинский Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/. – М.: Издательский центр «Академия», 2017. – 336с
21. Ю.Ю. Коваленко. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебное пособие / – М.: Горячая линия – Телеком, 2015.
22. Электронный конспект лекций «Инженерно-техническая защита информации». Составитель: И.Н. Драч, преподаватель ГБОУ СПО РО «РКСИ»
23. Электронный конспект лекций «Криптографическая защита информации». Составитель: Шигаева С.В., преподаватель ГБОУ СПО РО «РКСИ»
24. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2015.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.
25. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2015
26. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2016
27. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности: учебник: Рекомендовано УМО, 2019. - 192с.
28. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2015. – 416 с.
29. Архитектура ЭВМ и вычислительных систем: Учебник / Максимов Н.В., Партыка Т.Л., Попов И.И., - 5-е изд., перераб. и доп. - М.:Форум, НИЦ ИНФРА-М, 2016. - 512 с.: 60х90 1/16. - (Профессиональное образование) (Переплёт 7БЦ) ISBN 978-5-91134-742-0
30. Информатика: учебник / И.И. Сергеева, А.А. Музалевская, Н.В. Тарасова. — 2-е изд., перераб. и доп. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 384 с. — (Профессиональное образование).
31. Плотникова Н.Г. Информатика и информационно-коммуникационные технологии (ИКТ): Учеб. пособие. — М.: РИОР: ИНФРА-М, 2017. — 124 с. — (Среднее профессиональное образование). — www.dx.doi.org/10.12737/11561.
32. Практикум по информатике. Компьютерная графика и web-дизайн: учеб. пособие / Т.И. Немцова, Ю.В. Назарова ; под ред. Л.Г. Гагариной. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 288 с. + Доп. материалы [Электронный ресурс; Режим доступа <http://www.znanium.com>]. — (Профессиональное образование).

Дополнительные источники:

1. Березин О.К., Костиков В.Г., Шахнов В.А. Источники электропитания радиоэлектронной аппаратуры. Издание 4-е, перераб. и доп. - М: «Три Л», 2015.
2. Костиков В.Г., Парфенов Е.М., Шахнов В.А. Источники электропитания электронных средств. Схемотехника и конструирование: Учебник для вузов. – 3-е изд. – М.: Горячая линия – Телеком, 2019.
3. Источники электропитания радиоэлектронной аппаратуры: Справочник/ Г.С. Найвельт, К.Б. Мазель, Ч.И. Хусаинов и др.; Под ред. Г.С. Найвельта. – М.: Радио и связь, 2016.
4. Гейтенко Е.Н. Источники вторичного электропитания. Схемотехника и расчет. Учебное пособие. – М. СОЛОН-ПРЕСС, 2019.
5. Руководство администратора Криптон-замок
6. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: учеб. Пособие для студ. Высш. Учеб. Заведений – М.: Издательский дом «Академия», 2016. – 240с.
7. Торокин А.А. Инженерно-техническая защита информации: учебное пособие для студентов, обучающихся по специальностям в обл. информ. Безопасности –М.:Гелиос АРВ, 2015 – 960с.: ил. – ISBN 5-85438-140-0.
8. Руководство администратора ППКОП «Астра»
9. Руководство администратора КТМ-256
10. Учебное пособие Структурированная кабельная система NIKOMAX»
11. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- ☐ 12. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- ☐ 13. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
- ☐ 14. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
- ☐ 15. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
- ☐ 16. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
- ☐ 17. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
- ☐ 18. 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».
- ☐ 19. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
- ☐ 20. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
- ☐ 21. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.
- ☐ 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 недеklarированных 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 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 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
- 54 Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
- 55 ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
- 56 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
- 57 Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
- 58 Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.
- 59. Информатика, автоматизированные информационные технологии и системы: Учебник / В.А. Гвоздева. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015. - 544 с.: ил.; 60х90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0449-7
- 60. Информационные технологии: Учебное пособие / Л.Г. Гагарина, Я.О. Теплова, Е.Л. Румянцева и др.; Под ред. Л.Г. Гагариной - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015. - 320 с.: 60х90 1/16. - (Профессиональное образование). (п) ISBN 978-5-8199-0608-8, 400 экз.
- 61. Практикум по MicrosoftOffice 2007 (Word, Excel, Access), PhotoShop: Учебно-методическое пособие / Л.В. Кравченко. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 168 с.: 70х100 1/16. - (ПО). (о) ISBN 978-5-00091-008-5, 500 экз.
- 62. Сборник задач и упражнений по информатике: Учебное пособие/В.Д.Колдаев, под ред. Л.Г.Гагариной - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2015. - 256 с.: 60х90 1/16. - (Профессиональное образование) (Переплёт) ISBN 978-5-8199-0322-3, 200 экз.

Интернет ресурсы:

1. Электронно-библиотечная система [Электронный ресурс] – режим доступа: <http://znanium.com/> (2019).
2. <http://www.fstec.ru> сайт ФСТЭК РФ

3. <http://www.ancad.ru> сайт компании АНКАД
4. <https://www.cryptopro.ru/> сайт компании КриптоПро
5. <https://infotecs.ru/> сайт ОАО «ИнфоТеКС»